Some Results on Combinatorial Batch Codes and Permutation Binomials over Finite Fields

A thesis submitted in partial fulfillment for the
degree of Doctor of Philosophy
in Computer Science
by

Srimanta Bhattacharya

under the supervision of

Professor Bimal Roy

APPLIED STATISTICS UNIT

INDIAN STATISTICAL INSTITUTE

Kolkata, India.

Dedicated to my family members

and

in memoriam Prof. Dhrubojyoti Bhattacharya

Acknowledgements

I take this opportunity to gratefully acknowledge help, support, and motivation (direct or indirect) I received for this work.

I am indebted to my supervisor, Prof. Bimal Roy, for initiating me in the area of my research, for providing encouragement, help, and support whenever I needed, even during his difficult times. The independence he afforded me to conduct my research is invaluable.

I am also indebted to Prof. Palash Sarkar and Prof. Subhamoy Maitra for their numerous academic help and advices (most of which I could not live up to) starting from my M. Tech years.

I thank all my collaborators. Dr. Niranjan Balachandran has been more than a collaborator. His involvement in terms of discussions and advices has been vital for my research.

I am grateful to Dr. Mridul Nandi for his time and patience for some of the most engaging academic discussions I had during this period and also for his various other helps and suggestions. My sincere thanks to Dr. Kishan Chand Gupta for his time and for the interest he took in my overall affairs. His frequent iteractions helped me tide myself over the not-so-good times of my research.

I wholeheartedly thank past and present CRG members, whom I had the opportunity to work / interact with (with much pleasure and joy) - Dr. Ayineedi Venkateswarlu, Dr. Avishek Adhikari, Dr. Prem Laxman Das, Dr. Sumanta Sarkar, Dr. Somitra Sanadhya, Dr. Goutam Paul, Dr. Mrinal Nandi, Dr. Prabal Paul, Dr. Anupama Panigrahi, Sushmita, Mahabir, Pinaki, Santanu, Rishiraj, Sumit, Shashwat, Sourav, Sanjay, Butu, Somindu, Shashank, Raju (ASU), Indranil, Subhodeep, Tapas, Nilanjan, Avik, Kaushik, Pratyay, Binanda, Satrajit, Anubhab, Atanu, Sabyasachi. Their help and support have been far too wide.

I owe my gratitude to Prof. N. M. Singhi and Dr. Amitava Bhattacharya of TIFR, Mumbai for their kind patience and time for a month long discussion. I can not thank them more for hosting me with kind cordiality. I thank Mr. Mohit Garg of TIFR for many long discussions which broadened my perspective on the subject of my research.

I thank Prof. Yuval Ishai, Prof. David Gunderson, Prof. Zsolt Tuza and Prof. Csilla Bujtás for sending their unpublished manuscripts.

At various points, I had the opportunity to have short discussions on various problems related to my research with Prof. Jaikumar Radhakrishnan, Prof. Alexander Pott, Prof. Noga Alon, Prof. Zsolt Tuza, Prof. Csilla Bujtás, Prof. Sandip Sen, Prof. Dhruv Mubayi, Dr. Arnab Bhattacharyya. I thank all of them for their interest and their time and patience.

I thank Dr. Arijit Bishnu of ACMU for allowing me to attend some of his very well-taught courses. It helped me to attend different academic events that he arranged from time to time.

I thank Dr. Kaushik Majumdar of ISI, Bangalore for carefully reading part of my thesis and suggesting several corrections / changes which improved the quality of the thesis.

I thank instructors of my M. Tech coursework and my batchmates for creating an environment that encouraged me to do research. Baidya went out of his way to help me on various occasions.

I thank ASU faculty and office members, and COEC office members for their help and support.

I fondly remember and gratefully acknowledge the contributions of Prof. Dhrubojyoti Bhattacharya, my mathematics teacher at the higher secondary level, to my overall academic development. This work is only a partial fulfillment of his wishes.

It has been a test of patience for my family members - especially my parents. They trudged this arduous stretch with helpless rigour. Through their sacrifices they ensured that my priorities are met, in whichever ways they could; the rest is *mea culpa*. This work is as much theirs as it is mine.

"…but the bullfight was so far from simple and I liked it so much that it was much too complicated for my then equipment for writing to deal with and, aside from four very short sketches, I was not able to write anything about it for five years — and I wish I would have waited ten. However, if I had waited long enough I probably never would have written anything at all since there is a tendency when you really begin to learn something about a thing not to want to write about it but rather to keep on learning about it always and at no time, unless you are very egotistical, which, of course, accounts for many books, will you be able to say: now I know all about this and will write about it. Certainly I do not say that now; every year I know there is more to learn, but I know some things which may be interesting now, and I may be away from the bullfights for a long time and I might as well write what I know about them now."

-Ernest Hemingway
(from *Death in the afternoon*)

Contents

Overview

In this thesis, we study *combinatorial batch codes* (CBCs) and *permutation binomials* (PBs) over finite fields of even characteristic. Our primary motivation for considering these problems comes from their importance in cryptography. CBCs are replication based variants of batch codes, which were introduced in [IKOS04a] as a tool for reducing the computational overhead of *private information retrieval* protocols (a cryptographic primitive). On the other hand, permutation polynomials, with favourable cryptographic properties, have applications in symmetric key encryption schemes, especially in block ciphers.

Moreover, these two objects are interesting in their own right, and they have connections with other important combinatorial objects. CBCs are much similar to *unbalanced expanders*, a much studied combinatorial object having numerous applications in theoretical computer science. On the other hand, the specific class of PBs that we consider in this work, are intimately related to *orthomorphisms*. Orthomorphisms are relevant in the construction of *mutually orthogonal latin squares*, a classical combinatorial objects having applications in design of statistical experiments. These aspects motivate us to explore theoretical properties of CBCs and PBs over finite fields.

However, these two objects are inherently widely different; CBCs are purely combinatorial objects, and PBs are algebraic entities. So, we explore these two objects independently in two different parts, where our entire focus lies in exploring theoretical aspects of these objects. In Part I, we consider CBCs. There, we provide bounds on the parameters of CBCs and obtain explicit constructions of optimal CBCs. In Part II, we consider PBs over finite fields. There, we obtain explicit characterization and enumeration of subclasses of PBs under certain restrictions. Next, we describe these two parts in more detail.

Part I

In Part I of the thesis, we consider CBCs. This part is divided into four chapters.

1. In Chapter 1, we give introductory details on CBCs. There, we discuss basic setup and problems of CBCs that we consider in subsequent chapters. To motivate the discussion we begin with a brief description of batch codes.

   More detailed discussion on general batch codes is deferred till Appendix C. There, we stress their practical significance in the area of cryptography and load balancing.

   We point out that Appendix C is provided only for a general overview of batch codes. Its content is not required for understanding CBCs, discussed in the rest of this thesis (Chapters 1-4).

2. In Chapter 2, we consider the problem of finding minimum value of total storage of a CBC for given values of other parameters. There, we give a general lower bound on the total storage. We also obtain explicit constructions of optimal CBCs (i.e., CBCs that meet the stated lower bound). This partly answers an open question posed in [PSW09]. Also, one of our constructions establishes a connection between CBCs and constant weight codes.

   Results from this chapter have been published in [BRR12].

3. In Chapter 3, we consider the problem of obtaining the value of maximum number of input data items of uniform CBCs for given values of other parameters. We pose the problem as a *hypergraph Turán type problem*. Subsequently, we obtain upper bound on the order of magnitude of number of input data items. With respect to degree of uniformity (a parameter of uniform CBCs), this bound is best possible. This is shown by an explicit construction of uniform CBCs, where the number of input data items have asymptotically optimal order of magnitude. Several results pertaining to 2-uniform case are also presented.

   Results from this chapter have been published in [BB14].

4. In Chapter 4, we present globally explicit construction of uniform and almost regular CBCs. We derandomize a randomized construction of uniform CBCs, presented in [IKOS04a], to obtain our construction. Order of magnitude of input data items for the constructed CBCs is satisfactorily close to corresponding upper bound. More importantly, this construction, in terms of its explicitness, fills the void where no previous construction, with similar order of magnitude of input data items, is known. Also, prior to this, CBCs, that are both regular and uniform, have not been considered.

   Results from this chapter have been published in [Bha15].

In Appendices A and B, we formally state the notions and terminology from graph/hypergraph theory and coding theory that we use in this part of the thesis; though their use is fairly standard in the literature.

Bibliography I is the bibliography for Part I.

Part II

Part II of the thesis comprises of a single chapter, where we consider cyclotomic mapping PBs over $\mathbb{F}_{2^n}$. More specifically, we study two classes of PBs of the form $x^{\frac{2^n-1}{2^t-1}+1} + ax$ over $\mathbb{F}_{2^n}$ under certain restrictions. For one class of binomials we provide explicit characterization (necessary and sufficient conditions), i.e., characterization, which can be computed efficiently by a deterministic algorithm. For another class, we provide enumeration results. In both the cases, our results are under the restriction that a belong to certain subfields of $\mathbb{F}_{2^n}$.

To set proper context for our results we briefly discuss relevant aspects of permutation polynomials, cyclotomic mapping polynomials, and orthomorphisms. This includes their practical significance, especially in the areas of cryptography and combinatorial designs. We formalize the notion of explicit characterization of permutation polynomials in terms of computational complexity. We discuss existing results, which are relevant to the specific cases considered by us.

In Appendix D, we provide proofs of some known results discussed in Chapter 5. Also, we briefly describe relation between orthomorphisms and latin squares.

Results from this part have been published in [SBÇ12, BS15].

Bibliography II is the bibliography for Part II.

Part I

Combinatorial Batch Codes

Notation Summary For Part I

In this part of the thesis, we will use the following asymptotic notations.

Let f and g be functions of variable n. Then we write

- $f = O(g)$ if there is an absolute constant c such that $|f(n)|/|g(n)| \leq c$ for sufficiently large n,
- $f = o(g)$ if $\lim_{n\to\infty} f(n)/g(n) = 0$,
- $f = \Omega(g)$ if $g = O(f)$,
- $f = \Theta(g)$ if $f = O(g)$ and $g = O(f)$,
- $f \sim g$ if $f = (1 + o(1))g$,
- $f \lesssim g$ if $\limsup_{n\to\infty} f(n)/g(n) \leq 1$.

Chapter 1

Combinatorial Batch Codes: Introductory Details

Historically coding theory has been concerned with design of good codes, i.e., codes having good error-correcting capabilities with efficient encoding and decoding algorithms. However, in recent times, especially in the last two decades, the field has seen rapid and significant emergence of new characterizations and paradigms like *local decodability, local correctability, local testability, non-malleability*, etc., and also new families of codes like Expander codes, Parvaresh-Vardy codes, Matching vector codes, Multiplicity codes, etc. Much of the recent developments is motivated by applications in the domains of complexity theory and cryptography.

Batch codes were introduced in [IKOS04a] as an abstraction of a particular distributed database problem. It has strong practical and theoretical motivations. In this part of the thesis, we consider replication based variants of batch codes, known as *combinatorial batch codes* (CBCs). As we explore multiple aspects of CBCs, our presentation is divided into chapters. We make each chapter self-contained in terms of preliminaries and background required to understand the particular aspect treated in the chapter. To keep things in context, we introduce essential and relevant ideas when required. At various places in this part of the

thesis, we use terminology from coding theory and graph theory. Though the notions and terminology are fairly standard, in order to avoid any confusion, we formally define and describe them in Appendices A and B.

In this chapter, we discuss introductory details of CBCs. We formulate CBCs in appropriate setting and discuss the problems that we consider in subsequent chapters. However, to motivate the discussion we begin with a brief introduction to general batch codes. Somewhat more detailed discussion on various aspects of general batch codes, not essentially relevant to CBCs or more particularly to our contribution in this thesis, is deferred till Appendix C. It is left to the reader's discretion to go through that part.

1.1 BATCH CODES

An (n, N, k, m, t)-*batch code* abstracts the following data distribution problem.

> ***Batch code problem.*** [1] n data items are to be distributed among m servers in such a way that any k of the n items can be retrieved by reading at most t items from each server, and the total amount of storage across m servers is bounded by N.

Here, we state the following points regarding the above formulation.

1. In the sequel, we will refer to the parameter k in the above problem as *retrievability parameter*.

2. Although in [IKOS04a], batch codes were defined for general t, the case $t = 1$ seems to capture the crux of the problem. Hence, this case is exclusively treated in the literature (with the exception of [BT12]). In this work, we also consider the case $t = 1$ only and we will not explicitly mention t as a parameter. So, an (n, N, k, m)-batch code should be understood as $(n, N, k, m, t = 1)$-batch code. In Corollary C.2 of Appendix C, we list some straightforward relations between (n, N, k, m, t)-batch codes and (n, N, k, m)-batch codes.

[1] Refer to Appendix C for a formal definition of batch codes formulated in the language of coding theory.

Example 1.1 ((**15, 20, 2, 4**)-***Batch code***)**.** Consider distribution of $n = 15$ data items $x_1, \ldots, x_{15} \in \{0,1\}$ among $m = 4$ servers $S_1, \ldots, S_4$, such that any $k = 2$ items can be retrieved by reading at most $t = 1$ item from each server. This can be achieved by replicating each of the 15 items in all the servers. This trivial arrangement requires $N = 15 \times 4 = 60$ bits of storage. To improve the situation we employ the following method. We store $x_1, \ldots, x_5$ in S_1, $x_6, \ldots, x_{10}$ in S_2, $x_{11}, \ldots, x_{15}$ in S_3, and finally we store $x_1 \oplus x_6 \oplus x_{11}, \ldots, x_5 \oplus x_{10} \oplus x_{15}$ in S_4, where (and henceforth) $\oplus$ is the binary 'xor' operator. It can be observed that any 2 of the 15 elements can be retrieved by reading at most 1 element from each server. For example, to retrieve $\{x_4, x_5\}$ (i.e., to execute the query $\{4,5\}$), x_4 is read from S_1, x_{10} is read from S_2, x_{15} is read from S_3, and $x_5 \oplus x_{10} \oplus x_{15}$ is read from S_4. Now, with x_4 already obtained from S_1, x_5 is obtained as $x_5 = (x_{10}) \oplus (x_{15}) \oplus (x_5 \oplus x_{10} \oplus x_{15})$. In this case, the total storage is $N = 4 \times 5 = 20$ bits.

Remark 1.1. In fact, Example 1.1 is an example of *multiset batch codes* (see Appendix C), which supports the following stronger form of retrieval: in this case, we can retrieve a multiset $\{i, i\}, i \in \{1, \ldots, 15\}$ in such a way that the sets of servers queried for individual items form a partition of the entire set of servers. For example, to retrieve $\{8,8\}$ in Example 1.1, x_8 is read from S_2, x_3 is read from S_1, x_{13} is read from S_3, and $x_3 \oplus x_8 \oplus x_{13}$ is read from S_4. With one x_8 already obtained from S_2, the other x_8 can be obtained as $x_8 = (x_3) \oplus (x_{13}) \oplus (x_3 \oplus x_8 \oplus x_{13})$. Now, the sets of servers $\{S_2\}, \{S_1, S_3, S_4\}$ form the partition.

Batch codes were introduced in [IKOS04a]. Primary motivation behind their introduction was amortization of computational work done by servers during execution of *private information retrieval* (PIR) protocol. The authors have shown that these codes can be used to batch several PIR queries together while limiting total storage across servers (see [IKOS04a] for more details). Also, it can be seen from the above description that these codes can have potential application in a distributed database scenario. There, these codes can be used to distribute queries among participating servers while optimizing total storage. In Appendix C, we discuss these practical aspects in greater detail.

On the theoretical side, batch codes resemble other combinatorial objects like *locally decodable codes*, *expanders*, etc. Also, there is similarity with Rabin's *information dispersal* ([Rab89]). Below, we highlight this similarity, since it is immediate from the problem description of batch codes. Relations with expanders and locally decodable codes will be discussed later at appropriate places.

Relation with information dispersal. Informally, in an information dispersal scheme, a database $\mathcal{X}$ is distributed among n servers in such a way that the entire database can be reconstructed by reading from $m(< n)$ servers; the objective here is to minimize total storage across n servers. So, in both cases, the idea is to distribute a database in a way that facilitates its reconstruction; and in both the cases it is desirable to minimize the total storage across all the participating servers. However, in case of information dispersal, the goal is to achieve fault-tolerance and reconstruction of the entire database. While batch codes facilitate partial reconstruction of database by limiting the amount of retrieved information from each server; fault-tolerance is not an inherent objective of batch codes.

These similarities and dissimilarities, which are also present in the case of expanders and locally-decodable codes, make batch codes unique and intriguing. Similarities with other objects make batch codes theoretically important. On the other hand, differences make it difficult to set up a satisfactory and meaningful correspondence of batch codes with these objects in terms of parameters. In particular, it seems unlikely that existing bounds and constructions of expanders, locally decodable codes, etc., can be used in the context of batch codes.

1.2 COMBINATORIAL BATCH CODES

CBCs are replication based batch codes. In this case, each of the N stored data items is a copy of one of the n input data items. We illustrate this in the example of Figure 1.1, where we consider a $(7, 10, 4, 6)$-CBC. It can be checked that any 4 of the 7 data items can be retrieved by reading at most 1 item from each server.

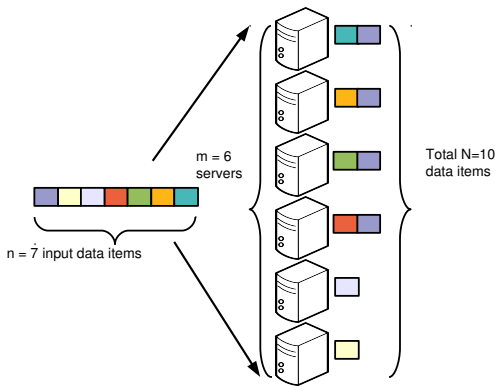

FIGURE 1.1: $(7, 10, 4, 6)$-CBC

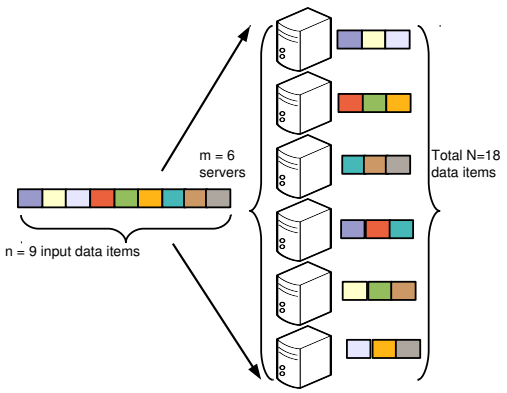

FIGURE 1.2: 2-uniform $(9, 18, 5, 6)$-CBC

Advantage of CBCs is clear from their formulation; storage and retrieval of data items are simple for CBCs. However, the requirement to store data items without any modification results in increased total storage (N). For example, below we show that a CBC with parameters from Example 1.1 can not exist.

Proposition 1.2. *A* $(15, 20, 2, 4)$*-CBC is not possible.*

Proof. Since the total storage (N) is 20, we observe that at least 10 input data items have single instances as stored data items in 4 servers. So, one of the 4 servers stores at least 3 of these 10 items. Now, any 2 of these 3 items can not be retrieved, as at most one item can be read from each server. □

The requirement to store data items without any modification makes CBCs purely combinatorial objects. As combinatorial objects CBCs are very interesting, and they have received considerable attention in recent literature ([PSW09, BKMS10a, BT11c, BT11b, BT15, SG14, BRR12, BB14]). Next, we formalize CBCs in the setting of a bipartite graph.

Let $\mathcal{C}$ be an (n, N, k, m)-CBC, with the set of input data items $\{x_1, \ldots, x_n\}$ and the set of servers $\{s_1, \ldots, s_m\}$. We represent $\mathcal{C}$ as a bipartite graph $\mathcal{G}_C = (\mathcal{L}, \mathcal{R}, \mathcal{E})$. Set of left vertices $\mathcal{L}$ represents $|\mathcal{L}| = n$ input data items, where vertex $u_i \in \mathcal{L}$ represents data item $x_i, 1 \leq i \leq n$. Set of right vertices $\mathcal{R}$ represents $|\mathcal{R}| = m$ servers, where vertex $v_j \in \mathcal{R}$ represents server $s_j, 1 \leq j \leq m$. $(u_i, v_j) \in \mathcal{E}$ is an edge in $\mathcal{G}_C$ if the data item x_i is stored in server s_j. Since the total storage is N, it follows that $\sum_{u \in \mathcal{L}} deg(u) = \sum_{v \in \mathcal{R}} deg(v) = |\mathcal{E}| = N$, where $deg(.)$ is the degree of a vertex in $\mathcal{G}_C$. Now, we observe that any subset $\{x_{i_1}, \ldots, x_{i_k}\}$ of k input data items can be retrieved by reading one item from each of k distinct servers $s_{i_1}, \ldots, s_{i_k}$ iff there are distinct $v_{i_1}, \ldots, v_{i_k} \in \mathcal{R}$ such that $v_{i_j} \in \Gamma(u_{i_j})$ for all $1 \leq j \leq k$, where $\Gamma(u_r)$, with $r \in \{1, \ldots, n\}$, is the *neighbourhood* of the vertex $u_r \in \mathcal{L}$. According to *Hall's theorem* (cf. [Bol86], pp. 6), this is equivalent to the condition that union of any j sets $\Gamma(u_{i_1}), \ldots \Gamma(u_{i_j})$ contains at least j elements for $1 \leq j \leq k$. These considerations lead naturally to the following theorem of [PSW09], which can also be thought as definition of a CBC.

Theorem 1.3 ([PSW09])**.** *A bipartite graph* $\mathcal{G}_C = (\mathcal{L}, \mathcal{R}, \mathcal{E})$ *represents an* (n, N, k, m)*-CBC* $\mathcal{C}$ *if and only if* $|\mathcal{L}| = n$, $|\mathcal{R}| = m$, $|\mathcal{E}| = N$, *and union of any collection of* j *sets* $\Gamma(u_{i_1}), \ldots, \Gamma(u_{i_j})$, *with* $\{u_{i_1}, \ldots, u_{i_j}\} \subset \mathcal{L}$, *contains at least* j *elements for* $1 \leq j \leq k$.

Remark 1.4. Formal definition of general batch codes, given in [IKOS04a] (see Appendix C), also involves *decoding algorithm* for the code. Here, we consider CBCs, which are a purely combinatorial subclass of general batch codes. Our focus is on bounds on parameters of CBCs and construction of optimal CBCs. Theorem 1.3, as a definition of a CBC, is sufficient for this purpose.

An (n, N, k, m)-CBC is called *c-uniform* if each of the n input data items is stored in exactly c servers, and it is called *ℓ-regular* if each of the m servers stores exactly ℓ data items. Rephrasing in the setting of bipartite graph, a CBC $\mathcal{G}_C = (\mathcal{L}, \mathcal{R}, \mathcal{E})$ is called *c-uniform* if for each $u \in \mathcal{L}$, $deg(u) = c$, and it is called ℓ-regular if for each $v \in R, deg(v) = \ell$. So, if an (n, N, k, m)-CBC is c-uniform then $N = cn$ and if it is ℓ-regular then $N = \ell m$. In Figure 1.2, we give an example of a 2-uniform $(9, 18, 5, 6)$-CBC, which is also 3-regular.

1.2.0.1 TWO PROBLEMS

In this thesis, we consider the following two problems related to CBCs. In fact, these are the only two problems that have so far been addressed in the literature.

1. Given n, m, k, we denote by $N(n, k, m)$ minimum value of N such that there is an (n, N, k, m)-CBC. An (n, N, k, m)-CBC, with $N = N(n, k, m)$ is termed *optimal*. For example, it can be formally shown that $N(7, 4, 6) = 10$. Hence, the $(7, 10, 4, 6)$-CBC, shown in Figure 1.1, is optimal.[2]

   However, it is challenging to find $N(n, k, m)$, in general, for given n, k, and m. Also, it is practically motivating to obtain explicit construction of optimal CBCs. We study this problem in Chapter 2, where we provide a general lower bound on $N(n, k, m)$. Also, we provide constructions of optimal (with respect to the obtained lower bound) and almost optimal CBCs for certain range of values of n (with respect to fixed values of m and k).

[2]Here, we note that an optimal CBC may not be unique.

2. Given m, c, k, we denote by $n(m, c, k)$ maximum value of n such that there is a c-uniform (n, cn, k, m)-CBC. A c-uniform (n, cn, k, m)-CBC, with $n = n(m, c, k)$ is termed *extremal*[3]. For example, it can be formally shown that $n(6, 2, 5) = 9$. In this case, the extremal CBC is obtained as follows. Partition the set of 6 servers into two groups of 3 servers each. Store each of the 9 input data items into any 2 of the 6 servers, one server from each group, in such a way that each of the 6 servers stores exactly 3 data items and no two data items are stored in the same set of 2 servers. In Figure 1.2, we give an example of an extremal 2-uniform $(9, 18, 5, 6)$-CBC (in fact, the CBC turns out to be 3-regular as well).

   However, finding $n(m, c, k)$ and constructing extremal CBCs, in general, is an extremely difficult problem, even for specific small values of the parameters. So, our goal is to understand the asymptotics of $n(m, c, k)$, where $n(m, c, k)$ is expressed as a function of m, with c, k constants independent of m. To be more precise, we are mostly concerned about the order of magnitude of $n(m, c, k)$. We study this problem in Chapter 3 and Chapter 4.

   In Chapter 3, we phrase the problem as an extremal hypergraph problem (Turán type problem). Subsequently, we obtain upper bound on $n(m, c, k)$. Also, we provide explicit construction of c-uniform (n, cn, k, m)-CBCs, where the order of magnitude of n is asymptotically optimal for certain range of values of c (with respect to k). For 2-uniform and 3-uniform CBCs we obtain several bounds (lower and upper) and explicit constructions.

   Explicit constructions of CBCs, obtained in Chapter 3, are for specific ranges of values of c and k. In Chapter 4, we obtain a general explicit construction of uniform and regular CBCs. Order of magnitude of n for the constructed CBCs is satisfactorily close to corresponding upper bound. More importantly, this construction, in terms of its explicitness, fills the void where no previous construction with similar parameters is known.

A note on setting and notation. In subsequent three chapters of this part, we consider the above mentioned problems of CBCs. We choose appropriate setting for each problem and we adjust notations accordingly. In Chapter 2, in order to simplify notation and description, we find it more convenient to represent a

[3]In the context of CBCs we will use the terms "extremal" and "optimal" interchangeably. In both cases, we refer to CBCs that meet certain bounds, which will be explicitly stated or clear from the context.

CBC as a set system $(\mathcal{S}, \mathcal{X})$, where $\mathcal{S}$ is the set of servers and $\mathcal{X}$ is a set of subsets of $\mathcal{S}$ which corresponds to the set of data items. In Chapter 3, we phrase the problem of obtaining $n(m, c, k)$ as an extremal hypergraph problem. There, we represent the CBC as a hypergraph $(\mathcal{V}, \mathcal{F})$, where $\mathcal{V}$ is the set of vertices of the hypergraph that correspond to the set of servers of the CBC, and $\mathcal{F}$ is the set of edges of the hypergraph that correspond to the set of data items of the CBC. In Chapter 4, we reuse the setting of bipartite graph described in this chapter. This inter-chapter variation of notation and setting simplifies description and notation for individual problems and makes it easier to relate our results to existing literature. However, to remove any confusion, in each chapter, we describe appropriate setting and notation with ample clarity.

In this part of thesis, we will use standard and basic results from probability theory. We refer the reader to [MR95] for relevant background on these results.

Chapter 2

Combinatorial Batch Codes: Lower Bound on Storage and Optimal Constructions

2.1 Introduction

In this chapter, we consider the problem of finding minimum value of total storage (N) of a CBC for given values of the number of data items (n), retrievability parameter (k), and number of servers (m). An (n, N, k, m)-CBC is termed *optimal* if N is minimum for given n, m, and k. We denote by $N(n, k, m)$ value of N of an optimal (n, N, k, m)-CBC. Finding $N(n, k, m)$ for given n, m, k and constructing corresponding optimal CBCs forms a practically important and interesting problem. For example, if $n \leq m$ then we trivially observe that $N(n, k, m) = n$; and for corresponding optimal CBC, n items are stored in any n out of m servers. But for $n \geq m + 1$, finding $N(n, k, m)$ is a fairly non-trivial problem.

In this section, we cover preliminaries, recall existing results, and state our contribution. In Section 2.2, we present proofs of our results. In Section 2.3, we conclude by reporting recent progress on this problem.

2.1.1 PRELIMINARIES

2.1.1.1 SETTING

As we have mentioned in Chapter 1, in order to simplify notation and description, in this chapter, we represent a CBC as a *set-system*. More formally, an (n, N, k, m)-CBC is a set system $(\mathcal{S}, \mathcal{X})$, where the ground set $\mathcal{S} = \{s_1, \ldots, s_m\}$ is the set of m servers, and $\mathcal{X} = \{X_1, X_2, \ldots, X_n\}$ is a set of n subsets of $\mathcal{S}$ such that $s_i \in X_j$ iff the j-th data item is stored in the i-th server. Next, we recall Theorem 1.3 of Chapter 1 for this setting.

Theorem 2.1 ([PSW09]). *A set-system $(\mathcal{S}, \mathcal{X})$ represents an (n, N, k, m)-CBC if and only if $|\mathcal{S}| = m$, $|\mathcal{X}| = n$, $\sum_{X \in \mathcal{X}} |X| = N$ and union of each collection of j sets $X_{i_1}, \ldots, X_{i_j} \subset \mathcal{X}$ contains at least j elements of $\mathcal{S}$ for $1 \leq j \leq k$.*

2.1.1.2 AN INEQUALITY

Now, we derive an inequality regarding the number of sets of different cardinalities in an (n, N, k, m)-CBC $(\mathcal{S}, \mathcal{X})$. This inequality is key to our proof of the lower bound on $N(n, k, m)$. The same inequality was obtained in [PSW09], as well as in [BT11c]. Here, our proof is somewhat different; we use probabilistic argument to derive the inequality. We also make certain additional observations.

Theorem 2.2. *Let $(\mathcal{S}, \mathcal{X})$ be an (n, N, k, m)-CBC, and A_i be the number of i element sets of $\mathcal{X}$. Then for any j, with $1 \leq j \leq k-1$, we have*

$$\sum_{i=1}^{j} \binom{m-i}{j-i} A_i \leq j \binom{m}{j}.$$

Proof. We pick uniformly at random a subset $\mathcal{S}' \subseteq \mathcal{S}$ of cardinality $j \leq k-1$. Let $\mathcal{X}_{\mathcal{S}'} = \{X \in \mathcal{X} | X \subseteq \mathcal{S}'\}$.

Now, for $X \in \mathcal{X}$, with $|X| = i$, probability that $X \subseteq \mathcal{S}'$ is given by

$$\mathbf{Pr}\{X \subseteq \mathcal{S}'\} = \frac{\binom{m-i}{j-i}}{\binom{m}{j}}.$$

Hence, expected value of $|\mathcal{X}_{\mathcal{S}'}|$ is given by

$$\mathbf{E}[|\mathcal{X}_{\mathcal{S}'}|] = \sum_{i=1}^{j} A_i \frac{\binom{m-i}{j-i}}{\binom{m}{j}},$$

where the expectation is taken over random choices for the subset $\mathcal{S}'$. Now, $\mathbf{E}[|\mathcal{X}_{\mathcal{S}'}|] \leq j$; otherwise, there is a subset $\mathcal{S}'' \subseteq \mathcal{S}$, with $|\mathcal{S}''| = j$, such that $|\mathcal{X}''_{\mathcal{S}}| > j$, but this violates Theorem 2.1. Hence, we have

$$\sum_{i=1}^{j} A_i \frac{\binom{m-i}{j-i}}{\binom{m}{j}} = \mathbf{E}[|\mathcal{X}_{\mathcal{S}'}|] \leq j.$$

So,

$$\sum_{i=1}^{j} A_i \binom{m-i}{j-i} \leq j \binom{m}{j} \tag{2.1}$$

□

So, considering every j in the range $1 \leq j \leq k-1$, we get $k-1$ inequalities like (2.1), each of which is satisfied by the (n, N, k, m)-CBC $(\mathcal{S}, \mathcal{X})$. However, we observe that these $k-1$ inequalities are not mutually independent. In fact, in the next lemma, we show that if $(j+1)$-th inequality is satisfied then j-th inequality is also satisfied.

Lemma 2.3. *Let $m \geq 3$ and $1 \leq j \leq k-2$. If*

$$\sum_{i=1}^{j+1} \binom{m-i}{j-i+1} A_i \leq (j+1) \binom{m}{j+1}$$

then

$$\sum_{i=1}^{j} \binom{m-i}{j-i} A_i \leq j \binom{m}{j}$$

.

Proof. We prove the contrapositive, i.e., we show that if

$$\sum_{i=1}^{j} \binom{m-i}{j-i} A_i > j \binom{m}{j} \tag{2.2}$$

then

$$\sum_{i=1}^{j+1} \binom{m-i}{j-i+1} A_i > (j+1)\binom{m}{j+1}.$$

Now, we have

$$\begin{aligned}\sum_{i=1}^{j+1} \binom{m-i}{j-i+1} A_i &= A_{j+1} + (m-j) \sum_{i=1}^{j} \frac{\binom{m-i}{j-i} A_i}{j-i+1} \\ &\geq A_{j+1} + \frac{m-j}{j} \sum_{i=1}^{j} \binom{m-i}{j-i} A_i. \end{aligned} \tag{2.3}$$

Now, from assumption (2.2) and from (2.3) we have

$$\sum_{i=1}^{j+1} \binom{m-i}{j-i+1} A_i > A_{j+1} + (m-j)\binom{m}{j} \geq (j+1)\binom{m}{j+1},$$

where, in the last step, we observe that $A_{j+1} \geq 0$ and $(m-j)\binom{m}{j} = (j+1)\binom{m}{j+1}$. □

Hence, it follows that if the $(k-1)$-th inequality, i.e.,

$$\sum_{i=1}^{k-1} \binom{m-i}{k-i-1} A_i \leq (k-1)\binom{m}{k-1}, \tag{2.4}$$

is satisfied then the remaining $k-2$ inequalities (obtained from (2.1) for $1 \leq j \leq k-2$) are also satisfied. That is, as necessary conditions for existence of an (n, N, k, m)-CBC, the other $k-2$ inequalities are redundant with respect to inequality (2.4). Hence, we exclude these $k-2$ inequalities from further consideration, and only use (2.4) as necessary condition for existence of an (n, N, k, m)-CBC. In [PSW09], the authors obtained inequality (2.4) in the proof of Theorem 2.1.1 by considering the case of $j = k-1$ only. Here, we have also shown that the other $k-2$ inequalities obtained from similar considerations are redundant; a fact which was not observed in [PSW09] and was not very evident in the first place.

2.1.2 EXISTING RESULTS

1. In [PSW09], the authors obtained $N(n,k,k)$, $N(m+1,k,m)$, and $N(n,k,m)$ for $n \geq (k-1)\binom{m}{k-1}$. More precisely, they have shown that

   (a) $N(n,k,k) = kn - k(k-1)$,

   (b) $N(m+1,k,m) = m+k$,

   (c) $N(n,k,m) = kn - (k-1)\binom{m}{k-1}$ for $n \geq (k-1)\binom{m}{k-1}$.

   The authors left the problem of finding $N(n,k,m)$ for $n < (k-1)\binom{m}{k-1}$ as an open problem.

2. In [BKMS10a] (see also [BKMS10b]), it was shown that

$$N(m+2,k,m) = \begin{cases} 2m + \lfloor \frac{m}{m-k+1} \rfloor & \text{if} \quad k \leq m \leq k+\sqrt{k}, \\ m+k-2+\lceil 2\sqrt{k+1} \rceil & \text{if} \quad m > k+\sqrt{k}. \end{cases}$$

   The authors proved the above results in the setting of transversal matroids. In [BT11a], the authors used a completely different technique to obtain these results. Moreover, in [BT11a], the authors also showed that

$$N(n,k,m) \leq 2m + (n-m-1)\left\lfloor \frac{k}{\lfloor \frac{m-k}{n-m-1} \rfloor + 1} \right\rfloor - b \text{ for all } m \geq k \geq 1,$$
$$n \geq m+2, \text{ where } b \text{ is the residue of } m-k \text{ modulo } n-m-1.$$

3. In [BT11c], the authors showed that for $\binom{m}{k-2} \leq n \leq (k-1)\binom{m}{k-1}$,

$$N(n,k,m) = n(k-1) - \left\lfloor \frac{(k-1)\binom{m}{k-1} - n}{m-k+1} \right\rfloor.$$

   This result was obtained in a simultaneous and independent work with our work ([BRR12]). However, they used a different technique. In a different direction, they also obtained $N(n,3,m)$ and $N(n,4,m)$ for all possible values of n and m.

2.1.3 OUR CONTRIBUTION

In this chapter, we obtain the following results.

1. We obtain a lower bound on $N(n,k,m)$ for n in the range $1 \leq n \leq (k-1)\binom{m}{k-1}$. More, precisely, our result is the following.

   Theorem 2.1.1. *Let $1 \leq n \leq (k-1)\binom{m}{k-1}$, and $1 \leq c \leq k-1$. Then for an (n,N,k,m)-CBC we have $N \geq nc - \left\lfloor \frac{(k-c)\left(\frac{(k-1)\binom{m}{c}}{\binom{k-1}{c}} - n\right)}{m-k+1} \right\rfloor$. The r.h.s. expression attains its maximum for least c such that $n \leq \frac{(k-1)\binom{m}{c}}{\binom{k-1}{c}}$.*

2. We provide explicit construction of optimal CBCs that meet the lower bound of Theorem 2.1.1 for n in the range $\binom{m}{k-2} \leq n \leq (k-1)\binom{m}{k-1}$. Exact value of $N(n,k,m)$ for this range is given by the following theorem.

   Theorem 2.1.2. *Let $\binom{m}{k-2} \leq n \leq (k-1)\binom{m}{k-1}$. Then we have $N(n,k,m) = n(k-1) - \left\lfloor \frac{(k-1)\binom{m}{k-1}-n}{m-k+1} \right\rfloor$.*

3. Using *binary constant weight codes*, we give explicit construction of CBCs for values of n in the range $\binom{m}{k-2} - (m-k+1)A(m,4,k-3) \leq n \leq \binom{m}{k-2}, k \geq 5$, where $A(m,4,k-3)$ is the maximum number of codewords of a binary constant weight code of length m, weight $k-3$, and Hamming distance 4. This construction yields optimal CBCs for approximately half of the values of n in this range. For the rest of the values of n, the construction yields almost optimal CBCs; for these CBCs, obtained value of N differs by one from the corresponding value of N given by the lower bound stated in (1) above. Below we state the theorem.

   Theorem 2.1.3. *Let $\binom{m}{k-2} - (m-k+1)A(m,4,k-3) \leq n \leq \binom{m}{k-2}$. Then*

$$N(n,k,m) = n(k-2) - \left\lfloor \frac{2\left(\binom{m}{k-2} - n\right)}{m-k+1} \right\rfloor$$
$$\text{for } 0 \leq \left(\binom{m}{k-2} - n\right) \mod (m-k+1) < \frac{m-k+1}{2}, \text{ and}$$
$$N(n,k,m) \leq n(k-2) - 2\left\lfloor \frac{\binom{m}{k-2} - n}{m-k+1} \right\rfloor$$
$$\text{for } \frac{m-k+1}{2} \leq \left(\binom{m}{k-2} - n\right) \mod (m-k+1) < m-k+1.$$

Constructions of optimal CBCs, stated in (2) and (3) above, partially settles the problem of finding $N(n,k,m)$ for $n < (k-1)\binom{m}{k-1}$, left open in [PSW09].

2.2 PROOFS

2.2.1 LOWER BOUND ON $N(n,k,m)$ FOR n IN THE RANGE $1 \le n \le (k-1)\binom{m}{k-1}$

We begin with the following lemma, where we derive an inequality to be used in Theorem 2.1.1.

Lemma 2.4. *Let $1 \le c < k \le m$ and $0 \le i \le k-1$. Then we have*

$$\frac{\binom{m-i}{k-1-i}}{\binom{m-c}{k-1-c}} - 1 \ge \frac{(m-k+1)(c-i)}{k-c}. \tag{2.5}$$

Proof. We note that both sides of (2.5) are equal for $i = c$ and $i = c-1$, and both sides decrease as i goes from 0 to $k-1$. Hence, it is sufficient to show that difference of values of l.h.s. of (2.5), for $i-1$ and i, is greater than or equal to $\frac{m-k+1}{k-c}$ for $2 \le i \le c-1$, and it is less than or equal to $\frac{m-k+1}{k-c}$ for $c+1 \le i \le k-1$. Now, we have

$$\frac{\binom{m-i+1}{k-i}}{\binom{m-c}{k-c-1}} - \frac{\binom{m-i}{k-i-1}}{\binom{m-c}{k-c-1}} = \frac{\frac{m-k+1}{k-i}\binom{m-i}{k-i-1}}{\binom{m-c}{k-c-1}} = \frac{\frac{m-k+1}{k-c}\binom{m-i}{k-i}}{\binom{m-c}{k-c}}.$$

Here, we note that for $c > i$,

$$\binom{m-i}{k-i}\binom{k-i}{c-i} = \binom{m-i}{c-i}\binom{m-c}{k-c},$$

and for $i > c$,

$$\binom{m-c}{k-c}\binom{k-c}{i-c} = \binom{m-c}{i-c}\binom{m-i}{k-i}.$$

In the above two cases, we use the identity $\binom{x}{y}\binom{y}{z} = \binom{x}{z}\binom{x-z}{y-z}$ for $x \ge y \ge z \ge 0$. Hence, it follows that

$$\frac{\frac{m-k+1}{k-c}\binom{m-i}{k-i}}{\binom{m-c}{k-c}} = \begin{cases} \dfrac{\frac{m-k+1}{k-c}\binom{m-i}{c-i}}{\binom{k-i}{c-i}} \ge \dfrac{m-k+1}{k-c}, & \text{when } c > i, \\ \dfrac{\frac{m-k+1}{k-c}\binom{k-c}{i-c}}{\binom{m-c}{i-c}} \le \dfrac{m-k+1}{k-c}, & \text{when } i > c\,. \end{cases}$$

Theorem 2.1.1. *Let* $1 \le n \le (k-1)\binom{m}{k-1}$, *and* $1 \le c \le k-1$. *Then for an* (n, N, k, m)-*CBC we have* $N \ge nc - \left\lfloor \frac{(k-c)\left(\frac{(k-1)\binom{m}{c}}{\binom{k-1}{c}} - n\right)}{m-k+1} \right\rfloor$. *The r.h.s. expression attains its maximum for least* c *such that* $n \le \frac{(k-1)\binom{m}{c}}{\binom{k-1}{c}}$.

Proof. Let $(\mathcal{S}, \mathcal{X})$ be an (n, N, k, m)-CBC. So, according to Theorem 2.1 union of any i sets, with $1 \le i \le k$, of $\mathcal{X}$ contains at least i elements. Therefore, it is sufficient for a set of $\mathcal{X}$ to be of size at most k. Hence, without loss of generality, we assume that each set of $\mathcal{X}$ is of cardinality at most k. Let A_i be the number of i-sets of $\mathcal{X}$. Then we have the following equation:

$$\sum_{i=1}^{k} A_i = n. \tag{2.6}$$

Next, $(\mathcal{S}, \mathcal{X})$ satisfies (2.4), which we recall below.

$$\sum_{i=1}^{k-1} \binom{m-i}{k-i-1} A_i \le (k-1)\binom{m}{k-1}. \tag{2.7}$$

We divide both sides of (2.7) by $\binom{m-c}{k-c-1}$ and then subtract (2.6) to have

$$\sum_{i=1}^{k-1} \left(\frac{\binom{m-i}{k-i-1}}{\binom{m-c}{k-c-1}} - 1 \right) A_i - A_k \le \frac{(k-1)\binom{m}{c}}{\binom{k-1}{c}} - n. \tag{2.8}$$

Employing (2.5) from Lemma 2.4 to (2.8), we get

$$\sum_{i=1}^{k-1} (c-i) A_i \le \frac{(k-c)\left(\frac{(k-1)\binom{m}{c}}{\binom{k-1}{c}} + A_k - n \right)}{m-k+1}. \tag{2.9}$$

Now, we have

$$N = \sum_{i=1}^{k} i A_i = nc - \sum_{i=1}^{k} (c-i) A_i. \tag{2.10}$$

Using (2.9) in (2.10), we get

$$N \ge nc - \frac{(k-c)\left(\frac{(k-1)\binom{m}{c}}{\binom{k-1}{c}} - n \right)}{m-k+1} + \frac{(k-c)(m-k)}{m-k+1} A_k. \tag{2.11}$$

Since $A_k \geq 0$, we have

$$N(n,k,m) \geq nc - \frac{(k-c)\left(\frac{(k-1)\binom{m}{c}}{\binom{k-1}{c}} - n\right)}{m-k+1}. \tag{2.12}$$

Difference between r.h.s. expressions of (2.12) for consecutive values c and $c+1$, where $1 \leq c \leq k-2$, is given by

$$\begin{aligned} nc - \frac{(k-c)\left(\frac{(k-1)\binom{m}{c}}{\binom{k-1}{c}} - n\right)}{m-k+1} - n(c+1) + \frac{(k-c-1)\left(\frac{(k-1)\binom{m}{c+1}}{\binom{k-1}{c+1}} - n\right)}{m-k+1} \\ = \frac{(m-k)\left(\frac{(k-1)\binom{m}{c}}{\binom{k-1}{c}} - n\right)}{m-k+1}. \end{aligned} \tag{2.13}$$

Here, we note that $\frac{\binom{m}{c}}{\binom{k-1}{c}}$ is an increasing function of c. Hence, second part of the theorem follows from from (2.13). Final expression of the l.h.s of the lower bound, involving floor operator, follows from (2.12) and the fact that $N(n,k,m)$ assumes integral values. □

2.2.2 CONSTRUCTION OF OPTIMAL CBCS FOR n IN THE RANGE $\binom{m}{k-2} \leq n \leq (k-1)\binom{m}{k-1}$

Let $\mathcal{S}$ be the set of servers, where $|\mathcal{S}| = m$. Now, for $k = 2$, the range of values of n is $1 \leq n \leq m$. As discussed in the beginning, for this range of values of n, we trivially have $N(n,k,m) = n$. Therefore, for the purpose of present construction, we consider cases where $m \geq k \geq 3$. Roughly, the construction is as follows. We start with a CBC $(\mathcal{S}, \mathcal{X}_i)$, in which $\mathcal{X}_i$ is a collection of $(k-1)$-subsets of $\mathcal{S}$. We also take an auxiliary collection $\mathcal{X}_a$ of distinct $(k-2)$-subsets of $\mathcal{S}$. From $\mathcal{X}_i$ we systematically delete $(k-1)$-sets and add to it $(k-2)$-sets from $\mathcal{X}_a$ to get the final collection $\mathcal{X}$. Below we describe the construction in more detail.

Construction. In the initial collection $\mathcal{X}_i$ there are $k-1$ copies of each of the $(k-1)$-subsets of $\mathcal{S}$. For the CBC to be constructed, we have $\binom{m}{k-2} \leq n \leq (k-1)\binom{m}{k-1}$. Hence, we have $0 \leq (k-1)\binom{m}{k-1} - n \leq (m-k+1)\binom{m}{k-2}$. The auxiliary collection $\mathcal{X}_a$ contains single copies of any $\left\lceil \frac{(k-1)\binom{m}{k-1}-n}{m-k+1} \right\rceil$ distinct $(k-2)$-subsets of $\mathcal{S}$. This is clearly possible for the range of values of $(k-1)\binom{m}{k-1} - n$. Next, we do the following $\left\lfloor \frac{(k-1)\binom{m}{k-1}-n}{m-k+1} \right\rfloor$ times.

1. Select a $(k-2)$-set from $\mathcal{X}_a$ and delete one copy of each of its $m-k+2$ supersets from $\mathcal{X}_i$. For each selected $(k-2)$-set of $\mathcal{X}_a$, we can always delete one copy of each of its $m-k+2$ supersets from $\mathcal{X}_i$ irrespective of previous deletions. This is because there are $k-1$ copies of each of the $(k-1)$-subsets of $\mathcal{S}$ in the initial collection $\mathcal{X}_i$. So, for a $(k-1)$-set of $\mathcal{X}_i$, its $k-1$ copies may be assumed to be assigned to its $k-1$ distinct $(k-2)$-subsets; one copy per subset. Therefore, for a $(k-2)$-set of $\mathcal{X}_a$, there corresponds a copy of each of its $m-k+2$ supersets in $\mathcal{X}_i$.

2. Add the $(k-2)$-set to the collection $\mathcal{X}_i$ and delete it from the auxiliary collection $\mathcal{X}_a$.

Finally, if $(m-k+1) \nmid ((k-1)\binom{m}{k-1}-n)$, then for the remaining $(k-2)$-set of $\mathcal{X}_a$, delete one copy of each of its $((k-1)\binom{m}{k-1}-n)-\left\lfloor \frac{(k-1)\binom{m}{k-1}-n}{m-k+1} \right\rfloor (m-k+1)$ supersets from $\mathcal{X}_i$. In the end, we get the final collection $\mathcal{X}$ of n subsets of $\mathcal{S}$. Before we prove correctness of the construction, we give an example to illustrate it.

Example 2.1. Let us take $m = 6, k = 4, n = 43$ and $\mathcal{S} = \{s_1, s_2, s_3, s_4, s_5, s_6\}$. Hence, in the initial collection $\mathcal{X}_i$ there are $k-1 = 3$ copies of each of the 20 3-subsets of $\mathcal{S}$. The auxiliary collection $\mathcal{X}_a$ contains $\left\lceil \frac{(k-1)\binom{m}{k-1}-n}{m-k+1} \right\rceil = 6$ 2-subsets of $\mathcal{S}$. Let the collection $\mathcal{X}_a$ be $(\{s_1, s_2\}, \{s_2, s_3\}, \{s_3, s_4\}, \{s_4, s_5\}, \{s_5, s_6\}, \{s_1, s_6\})$.

In step 1, we select the set $\{s_1, s_2\}$ from $\mathcal{X}_a$, delete a single copy of each of its $m-k+2 = 4$ supersets (i.e., $\{s_1, s_2, s_3\}, \{s_1, s_2, s_4\}, \{s_1, s_2, s_5\}, \{s_1, s_2, s_6\}$) from $\mathcal{X}_i$, add the set $\{s_1, s_2\}$ to $\mathcal{X}_i$, and delete it from $\mathcal{X}_a$. We repeat these steps for 4 other sets (let us assume $\{s_2, s_3\}, \{s_3, s_4\}, \{s_4, s_5\}, \{s_5, s_6\}$) of $\mathcal{X}_a$.

Finally, for the remaining set $\{s_1, s_6\}$, we delete two of its supersets $\{s_1, s_2, s_6\}$ and $\{s_1, s_3, s_6\}$ from collection $\mathcal{X}_i$. Table 5.1 shows the final collection $\mathcal{X}$. Next, we prove correctness of this construction.

Proof of correctness. First, we note that sets of $\mathcal{X}$ are of cardinality $k-1$ and $k-2$, where the $(k-2)$-sets are all distinct. Hence, it follows that union of i sets of $\mathcal{X}$ contains at least i elements for $1 \leq i \leq k-1$. Next, we observe that the collection $\mathcal{X}$ contains at most $k-1$ subsets of a $(k-1)$-set, which may possibly include one or more copies of the $(k-1)$-set itself. So, in a collection of k sets of $\mathcal{X}$ there can be at most $k-1$ subsets of a $(k-1)$-set. Hence, union of any k sets of $\mathcal{X}$ contains at least k elements. □

TABLE 2.1: Final collection $\mathcal{X}$ of Example 2.1

Subset	Number of copies	Subset	Number of copies
$\{s_1, s_2, s_3\}$	1	$\{s_2, s_3, s_6\}$	2
$\{s_1, s_2, s_4\}$	2	$\{s_2, s_4, s_6\}$	3
$\{s_1, s_2, s_5\}$	2	$\{s_2, s_5, s_6\}$	3
$\{s_1, s_2, s_6\}$	2	$\{s_3, s_4, s_5\}$	1
$\{s_1, s_3, s_4\}$	2	$\{s_3, s_4, s_6\}$	2
$\{s_1, s_3, s_5\}$	3	$\{s_3, s_5, s_6\}$	2
$\{s_1, s_3, s_6\}$	2	$\{s_4, s_5, s_6\}$	1
$\{s_1, s_4, s_5\}$	2	$\{s_1, s_2\}$	1
$\{s_1, s_4, s_6\}$	3	$\{s_2, s_3\}$	1
$\{s_1, s_5, s_6\}$	2	$\{s_3, s_4\}$	1
$\{s_2, s_3, s_4\}$	1	$\{s_4, s_5\}$	1
$\{s_2, s_3, s_5\}$	2	$\{s_5, s_6\}$	1
$\{s_1, s_4, s_6\}$	3	$\{s_2, s_3\}$	1
$\{s_1, s_5, s_6\}$	2	$\{s_3, s_4\}$	1
$\{s_2, s_3, s_4\}$	1	$\{s_4, s_5\}$	1
$\{s_2, s_3, s_5\}$	2	$\{s_5, s_6\}$	1

So, $(\mathcal{S}, \mathcal{X})$ is an (n, N, k, m)-CBC, where $N = \sum_{X \in \mathcal{X}} |X| = n(k-1) - \left\lfloor \frac{(k-1)\binom{m}{k-1} - n}{m-k+1} \right\rfloor$. Hence, following Theorem 2.1.1, it is an optimal CBC. Therefore, we have proved the following.

Theorem 2.1.2. *Let* $\binom{m}{k-2} \leq n \leq (k-1)\binom{m}{k-1}$. *Then we have* $N(n, k, m) = n(k-1) - \left\lfloor \frac{(k-1)\binom{m}{k-1} - n}{m-k+1} \right\rfloor$.

2.2.3 CONSTRUCTION OF OPTIMAL AND ALMOST OPTIMAL CBCS USING BINARY CONSTANT WEIGHT CODES

A binary constant weight code is a nonlinear code over $\mathbb{F}_2$, finite field of order 2, whose every codeword has same weight. In order to apply binary constant weight codes for construction of CBCs, we view codewords as characteristic vectors [1] of subsets. A w-subset of an n-set is identified with a codeword of length n and weight w, where the codeword is the characteristic vector of the subset. Thus, if distance between two codewords is d then symmetric difference between the two corresponding subsets is also d. We say that such a pair of subsets is *d distance apart*.

[1] Let $\mathcal{S}$ be an ℓ-set $\{s_1, s_2, \ldots, s_\ell\}$. For $I \subseteq \mathcal{S}$, *characteristic vector* of I is the vector $\chi_I = (c_1, c_2, \ldots, c_\ell) \in \mathbb{F}_2^\ell$ such that $c_i = 1$ iff $s_i \in I$, $1 \leq i \leq \ell$, where $\mathbb{F}_2$ is the finite field of order 2. So, a subset of a set can be naturally identified with its characteristic vector.

Let $A(n, 2d, w)$ denote maximum number of codewords of a binary constant weight code of length n, weight w, and minimum distance $2d$ [2] over field $\mathbb{F}_2$. Our construction of optimal and almost optimal CBCs is for the range of values of n, with $\binom{m}{k-2} - (m-k+1)A(m,4,k-3) \leq n \leq \binom{m}{k-2}$, where $k \geq 5$. To get an approximate idea of this range, we state few results from [GS80] regarding lower bound on $A(n, 2d, w)$. For improvements on these results and other relevant details of constant weight codes, we refer the reader to [BSSS90, AVZ00, BE10, Klo81, VPE89, SHP06].

Theorem 2.5 ([GS80]). $A(n, 4, w) \geq \frac{1}{n}\binom{n}{w}$.

For arbitrary d we note the following lower bound.

Theorem 2.6 ([GS80]). $A(n, 2d, w) \geq \frac{1}{q^{d-1}}\binom{n}{w}$, *where q is a prime power such that $q \geq n$.*

Theorem 2.6, along with Johnson's upper bound on the size of binary constant weight codes, implies the following asymptotic estimate of $A(n, 2d, w)$.

Theorem 2.7 ([GS80]). $\frac{n^{(w-d+1)}}{w!} \lesssim A(n, 2d, w) \lesssim \frac{(d-1)!n^{(w-d+1)}}{w!}$, *for w fixed as $n \to \infty$.*

For $d = 2$, Theorem 2.7 implies $A(n, 4, w) \sim \frac{n^{(w-d+1)}}{w!}$.

Construction. Our overall construction procedure, in this case, is similar to our previous construction; although, with a different initial collection $(\mathcal{X}_i)$ and auxiliary collection $(\mathcal{X}_a)$. Let $\mathcal{S}$ to be the set of servers with $|\mathcal{S}| = m$. Initial collection $\mathcal{X}_i$ consists of all the $\binom{m}{k-2}$ $(k-2)$-subsets of $\mathcal{S}$.

Range of possible values of n is $\binom{m}{k-2} - (m-k+1)A(m,4,k-3) \leq n \leq \binom{m}{k-2}$. Hence, we have $0 \leq \binom{m}{k-2} - n \leq (m-k+1)A(m,4,k-3)$. Unlike in the previous construction, our choice of auxiliary collection $(\mathcal{X}_a)$ of sets is not arbitrary. In this case, $\mathcal{X}_a$ is a collection of $\left\lceil \frac{\binom{m}{k-2}-n}{m-k+1} \right\rceil$ distinct $(k-3)$-subsets of $\mathcal{S}$, which are mutually minimum 4 distance apart. Our choice of the $(k-3)$-sets of $\mathcal{X}_a$ is guided by codewords of corresponding binary constant weight codes. This is possible for the range of values of $\binom{m}{k-2} - n$. Next, we do the following $\left\lfloor \frac{\binom{m}{k-2}-n}{m-k+1} \right\rfloor$ times.

[2] Here, we note that distance between two codewords of a constant weight code is always even.

1. Select a $(k-3)$-set from $\mathcal{X}_a$ and delete each of its $m-k+3$ supersets from $\mathcal{X}_i$. This can be done for each $(k-3)$-set of $\mathcal{X}_a$ irrespective of all the previous deletions. This is because $(k-3)$-sets of $\mathcal{X}_a$ are mutually minimum 4 distance apart. Hence, union of any two $(k-3)$-sets of $\mathcal{X}_a$ contains at least $k-1$ elements. Therefore, no two $(k-3)$-sets of $\mathcal{X}_a$ have the same $(k-2)$-set in $\mathcal{X}_i$ as superset.

2. Delete the $(k-3)$-set from $\mathcal{X}_a$ and add two copies of the set to $\mathcal{X}_i$.

Finally, if $(m-k+1) \nmid (\binom{m}{k-2} - n)$, then for the remaining $(k-3)$-set of $\mathcal{X}_a$, delete its $(\binom{m}{k-2} - n) - \left\lfloor \frac{\binom{m}{k-2}-n}{m-k+1} \right\rfloor (m-k+1)$ supersets from $\mathcal{X}_i$.

In the end, we get the final collection $\mathcal{X}$ of n subsets of $\mathcal{S}$.

Proof of correctness. Sets of the collection $\mathcal{X}$ are of cardinality $k-2$ and $k-3$. There are exactly two copies of a $(k-3)$-set, and the $(k-2)$-sets are all distinct. Also, following the choice of auxiliary collection $\mathcal{X}_a$, union of any two distinct $(k-3)$-sets contains at least $k-1$ elements. Therefore, union of $k-1$ sets of $\mathcal{X}$ contains at least $k-1$ elements for $k \geq 5$.

Now, we consider any collection $\mathcal{X}_k$ of k sets of $\mathcal{X}$. If union of the sets of $\mathcal{X}_k$ contains at least k elements then we are done. Otherwise, from the above, it follows that the union contains at least $k-1$ elements. Let us denote the set of these $k-1$ elements by X. Since union of k distinct $(k-2)$-sets contains at least k elements, $\mathcal{X}_k$ contains at least one $(k-3)$-set. Let the number of $(k-3)$-sets in $\mathcal{X}_k$ be r, where $1 \leq r \leq k$. Since there are exactly two copies of each $(k-3)$-set in $\mathcal{X}$, there are at least $\lceil \frac{r}{2} \rceil$ distinct $(k-3)$-sets in $\mathcal{X}_k$. Each of these $(k-3)$-sets has exactly two $(k-2)$-supersets, which are subsets of X. Now, from the choice of $\mathcal{X}_a$ it follows that no two distinct $(k-3)$-sets of $\mathcal{X}_k$ share the same $(k-2)$-superset that is a subset of X. Hence, there are at least $2\lceil \frac{r}{2} \rceil$ distinct $(k-2)$-subsets of X that are supersets of $(k-3)$-sets of $\mathcal{X}_k$. Also, there are $k-r$ distinct $(k-2)$-sets in $\mathcal{X}_k$ that are subsets of X, and are not supersets of any $(k-3)$-set of $\mathcal{X}_k$. Hence, there are at least $2\lceil \frac{r}{2} \rceil + k - r \geq k$ distinct $(k-2)$-subsets of X. But this is a contradiction, since X is a set of $k-1$ elements. □

So, $(\mathcal{S}, \mathcal{X})$ is an (n, N, k, m)-CBC, where $N = \sum_{X \in \mathcal{X}} |X| = n(k-2) - 2\left\lfloor \frac{\binom{m}{k-2}-n}{m-k+1} \right\rfloor$.

Now, we discuss optimality of this construction. We note that Theorem 2.1.1 implies the following lower bound.

$$N(n,k,m) \geq n(k-2) - \left\lfloor \frac{2\left(\binom{m}{k-2} - n\right)}{m-k+1} \right\rfloor, \tag{2.14}$$

for $n \leq \binom{m}{k-2}$. Hence, difference between value of N obtained from our construction and value of N given by the lower bound (2.14) for given values of n, m, and k is

$$\left(n(k-2) - 2\left\lfloor \frac{\binom{m}{k-2} - n}{m-k+1} \right\rfloor\right) - \left(n(k-2) - \left\lfloor \frac{2\left(\binom{m}{k-2} - n\right)}{m-k+1} \right\rfloor\right)$$

$$= \begin{cases} 0, & \text{when } 0 \leq \left(\binom{m}{k-2} - n\right) \mod (m-k+1) < \frac{m-k+1}{2}; \\ 1, & \text{when } \frac{m-k+1}{2} \leq \left(\binom{m}{k-2} - n\right) \mod (m-k+1) < m-k+1. \end{cases}$$

So, the construction yields optimal CBCs for approximately half of the values of n in the range $\binom{m}{k-2} - (m-k+1)A(m,4,k-3) \leq n \leq \binom{m}{k-2}$. For the rest of the values of n within this range, value of N for the constructed CBC differs by one from the value of N, given by the lower bound (2.14). Therefore, for these values of n constructed CBCs are almost optimal. More formally, we have proved the following result.

Theorem 2.1.3. *Let* $\binom{m}{k-2} - (m-k+1)A(m,4,k-3) \leq n \leq \binom{m}{k-2}$. *Then*

$$N(n,k,m) = n(k-2) - \left\lfloor \frac{2(\binom{m}{k-2} - n)}{m-k+1} \right\rfloor$$

$$\textit{for } 0 \leq \left(\binom{m}{k-2} - n\right) \mod (m-k+1) < \frac{m-k+1}{2}, \textit{ and}$$

$$N(n,k,m) \leq n(k-2) - 2\left\lfloor \frac{\binom{m}{k-2} - n}{m-k+1} \right\rfloor$$

$$\textit{for } \frac{m-k+1}{2} \leq \left(\binom{m}{k-2} - n\right) \mod (m-k+1) < m-k+1.$$

2.3 CONCLUSION AND SUBSEQUENT WORK

Along with the construction, given in Theorem 2.1.3, in [BRR12], we used constant weight codes for construction of c-uniform (n, cn, k, m)-CBCs. For these CBCs, we showed $n = \Omega(m^{2c-k+2})$. We do not discuss the result here, as the order of magnitude of n has been significantly improved by the constructions given in Chapter 3 and Chapter 4.

In this chapter, we have constructed optimal and almost optimal (n, N, k, m)-CBCs, where data items are stored in $\sim k$ servers, that is, for such a CBC $(\mathcal{S}, \mathcal{X})$, sets of $\mathcal{X}$ have cardinality $\sim k$. In a recent work ([SG14]), the authors have constructed optimal CBCs $(\mathcal{S}, \mathcal{X})$, where sets of $\mathcal{X}$ have cardinality $\sim \sqrt{k}$. More precisely, using *transversal designs*, they have constructed optimal (n, N, k, m)-CBCs, with $n = q^2 + q - 1, k = q^2 - q - 1, m = q^2 - q, N = q^3 - q$, where $q \geq 3$ is a prime power. For such a CBC $(\mathcal{S}, \mathcal{X})$, sets of $\mathcal{X}$ have cardinality $\in \{q, q-1\}$. We note that for these optimal CBCs, setting of parameters is relatively specific (e.g., in this case, $m = k + 1$). However, the important point is that, the construction shows that the lower bound on $N(n, k, m)$, obtained in Theorem 2.1.1, is tight for a rather different setting of parameters; namely, when the sets of $\mathcal{X}$ (for an (n, N, k, m)-CBC $(\mathcal{S}, \mathcal{X})$) have cardinality $\sim \sqrt{k}$.

Chapter 3

On an Extremal Hypergraph Problem Related to Combinatorial Batch Codes

3.1 Introduction

In this chapter, we consider the problem of obtaining the value of maximum number of input data items (n) of a uniform CBC for given values of the number of servers (m), retrievability parameter (k), and degree of uniformity (c). Given m, c, k, we denote by $n(m, c, k)$ maximum value of n such that there is a c-uniform (n, cn, k, m)-CBC. We term a c-uniform (n, cn, k, m)-CBC, with $n = n(m, c, k)$, *extremal*. As we mentioned in Chapter 1, finding the value of $n(m, c, k)$ is a very difficult problem, even for specific small values of m, c, and k. We view the problem as an extremal hypergraph problem, or more precisely, as a *hypergraph Turán type problem*. We obtain bounds on $n(m, c, k)$ and construct extremal (up to order of magnitude of n) CBCs. For certain ranges of values of parameters, our constructions improve on existing lower bounds on $n(m, c, k)$, which also includes an improvement on a non-constructive lower bound, obtained by Brown, Erdős, and Sós ([BES73]), for a degenerate extremal problem.

In this section, we cover the preliminaries, where we discuss basics of *Turán numbers* and *Turán density*. We formally phrase the problem of obtaining $n(m, c, k)$ as an extremal hypergraph problem, and make initial observations on the problem. Then we discuss existing results and state our contribution. Section 3.2 comprises of proofs of our results. Finally, we conclude in Section 3.3 by reporting subsequent progress made on this problem.

3.1.1 Preliminaries

3.1.1.1 Turán numbers and Turán density

Let $\mathcal{H}$ be a family of c-uniform hypergraphs. Maximum size of a c-uniform hypergraph on m[1] vertices, that does not contain a copy of any of the hypergraphs of $\mathcal{H}$ as a sub-hypergraph, is called *Turán number* of the family $\mathcal{H}$, and is denoted by $\text{ex}(m, \mathcal{H})$ [2]. A hypergraph (which may not be unique) on m vertices and with $\text{ex}(m, \mathcal{H})$ edges that does not contain a member of $\mathcal{H}$ is *extremal* for the family $\mathcal{H}$. Given a family $\mathcal{H}$ of hypergraphs determining $\text{ex}(m, \mathcal{H})$ and corresponding extremal hypergraph(s) is commonly termed *Turán type problem*, where the family $\mathcal{H}$ is called the *family of forbidden hypergraphs* for the problem. Turán type problems form one of the most interesting classes of extremal combinatorial problems.

One of the classical results in this area is due to Turán [Tur41], who determined $\text{ex}(m, K_t)$ and also the corresponding unique extremal graph.[3] This, however, is one of the very few exact results for this type of problems, which are known to be notoriously hard. For large number of families (even containing a single member) $\mathcal{F}$ of c-uniform hypergraphs, even the order of magnitude of $\text{ex}(m, \mathcal{F})$ is not known. For graphs, the situation is somewhat better due to the famous

[1] In order to maintain notational consistency throughout the thesis, we deviate from the standard notation of graph/ hypergraph literature. We denote by m, number of vertices and by n, number of edges of a graph / hypergraph. This is in exact contradiction to their standard use in graph / hypergraph literature.

[2] We do not include the degree of uniformity c in the notation as it is clear from the context, and does not create any confusion.

[3] Although the earliest known result in this area is due to Mantel [Man07], who solved the case for $t = 3$, i.e., for triangles.

Erdős-Stone -Simonovits theorem [ES46, ES66], which roughly asserts that

$$\mathrm{ex}(m,\mathcal{F}) = \left(\min_{G\in\mathcal{F}}\left(1-\frac{1}{\chi(G)-1}\right)+o(1)\right)\binom{m}{2}, \tag{3.1}$$

where $\chi(G)$ is the chromatic number of G. So, apart from the case when the family $\mathcal{F}$ contains a bipartite graph (which have chromatic number 2) the problem of determining the Turán number for graphs is settled as far as asymptotic is concerned.

For c-uniform hypergraphs, with $c \geq 3$, the problem is still very much open. There are no analogues of Turán's theorem or Erdős-Stone-Simonovits theorem for these hypergraphs, and result of general nature is almost missing. In fact, difficulty of Turán type problems in this setting can be gauged from the fact that even one of the basic non-trivial problems in this domain (famously known as *Turán's* $3-4$ *problem*), that of determining the Turán number of Tetrahedron, i.e., determining $\mathrm{ex}(m,K_4^3)$, is unsettled till date.[4] Since obtaining exact value of $\mathrm{ex}(m,\mathcal{H})$ is a difficult problem in general, it is natural to focus on the asymptotics of $\mathrm{ex}(m,\mathcal{H})$. In order to understand the asymptotics of $\mathrm{ex}(m,\mathcal{H})$, we consider the following two sub-problems.

– Determination of the order of magnitude of $\mathrm{ex}(m,\mathcal{H})$: Logically the first step towards understanding the asymptotics of $\mathrm{ex}(m,\mathcal{H})$ is to understand its order of magnitude, i.e., the value α such that $\mathrm{ex}(m,\mathcal{H}) = \Theta(m^\alpha)$. It is known that $\mathrm{ex}(m,\mathcal{H}) = o(m^c)$ if and only if the c-uniform family of forbidden hypergraphs $\mathcal{H}$ contains a member that is c-partite. However, given a description of the family $\mathcal{H}$, it may not be obvious whether the family contains a c-partite member. More interestingly, and almost always it is the case that when $\mathrm{ex}(m,\mathcal{H}) = o(m^c)$, determination of exact value α such that $\mathrm{ex}(m,\mathcal{H}) = \Theta(m^\alpha)$ becomes exceedingly challenging, even in the case of graphs. For this special case, the problem is known as *degenerate* extremal problem. There is a vast literature covering these types of problems. We refer the reader to [FS13] for a recent and extensive survey of degenerate extremal problems in the case of graphs.

[4] Erdős offered \$500 for a solution of this problem and \$1000 for solution of $\mathrm{ex}(m,K_t^c)$

– Determination of the leading coefficient of $\mathrm{ex}(m,\mathcal{H})$: Once the order of magnitude of $\mathrm{ex}(m,\mathcal{H})$ is determined, the next step is to obtain its leading coefficient. However, this is also a very difficult problem, even for c-uniform families $\mathcal{H}$ for which $\mathrm{ex}(m,\mathcal{H}) = \Theta(m^c)$. For such a family, the leading coefficient of $\mathrm{ex}(m,\mathcal{H})$ is expressed as *Turán density* of $\mathcal{H}$. More formally, for a c-uniform family $\mathcal{H}$, its Turán density, denoted by $\pi(\mathcal{H})$, is defined as (see [Kee11])

$$\pi(\mathcal{H}) \triangleq \lim_{m\to\infty} \frac{\mathrm{ex}(m,\mathcal{H})}{\binom{m}{c}}.$$

That the above limit exists was shown in [KNS64]. For a degenerate c-uniform family $\mathcal{H}$, i.e., for a family with $\mathrm{ex}(m,\mathcal{H}) = o(m^c)$, it immediately follows that $\pi(\mathcal{H}) = 0$. So, Turán density is meaningful only for a non-degenerate c-uniform family $\mathcal{H}$, and in this case, it immediately follows that $\mathrm{ex}(m,\mathcal{H}) \sim \pi(\mathcal{H})\binom{m}{c}$. There are only a few specific families for which Turán density is known (see [Kee11] for a detailed and updated survey on progress in this area, mostly for small families and for $c = 3$ and 4 cases). However, the problem, in general, is far from being solved.

We refer the reader to (somewhat old) surveys [Fűr91, Sid95], and more recent [Sud10] for further details and results on Turán type problems.

3.1.1.2 Combinatorial batch codes and an extremal problem

Setting and notation. In this chapter, we consider the problem of finding maximum number of input data items (n) of a uniform CBC for given values of the number of servers (m), retrievability parameter (k), and degree of uniformity (c). We represent a uniform CBC by a uniform hypergraph and pose the problem as a hypergraph Turán type problem.

Following their common use in literature, we will use the notation $\mathrm{ex}(m,\mathcal{H})$ to denote Turán number of the family $\mathcal{H}$ taken over simple hypergraphs only, i.e., to denote maximum size of a simple hypergraph without containing any member of $\mathcal{H}$. We use $\mathrm{ex}^*(m,\mathcal{H})$ when we allow considered hypergraphs to have repeated edges,i.e., we denote by $\mathrm{ex}^*(m,\mathcal{H})$ maximum size of a hypergraph with repeated edges that does not contain any member of $\mathcal{H}$.

Problem definition and basic observations. We represent a c-uniform (n, cn, k, m)-CBC by a c-uniform hypergraph $(\mathcal{V}, \mathcal{F})$, where the set of vertices $\mathcal{V}$, with $|\mathcal{V}| = m$, represents the set of m servers, and the set of edges $\mathcal{F}$, with $|\mathcal{F}| = n$, represents the set of n data items. Edge $F_i \in \mathcal{F}$ contains vertex $v_j \in \mathcal{V}$ if and only if i-th data item is stored in j-th server. Now, we recall Theorem 1.3 of Chapter 1, which serves as a definition of a CBC in this setting.

Theorem 3.1 ([PSW09]). *A c-uniform hypergraph $(\mathcal{V}, \mathcal{F})$ represents a c-uniform (n, cn, k, m)-CBC if and only if $|\mathcal{V}| = m$, $|\mathcal{F}| = n$, $\sum_{F\in\mathcal{F}} |F| = cn$, and every collection of i edges from $\mathcal{F}$ contains at least i vertices for $1 \leq i \leq k$.*

Now, we formally state the problem, which we consider in this chapter, in the setting of hypergraphs.

> *Let m, c, k be positive integers such that $3 \leq k < n$ and $2 \leq c \leq k-1$. Determine $n(m, c, k)$, i.e., the maximum number of edges a c-uniform hypergraph on m vertices can have subject to the condition that any collection of i edges spans at least i vertices for $1 \leq i \leq k$.*

This is a Turán type problem, where we have the following family of forbidden hypergraphs:

$$\mathcal{G}^c(k) = \{H | H \text{ is a } c\text{-uniform hypergraph with } i \text{ edges and } < i \text{ vertices for } 1 \leq i \leq k\}. \tag{3.2}$$

We are interested in the order of magnitude of $n(m, c, k) = \mathrm{ex}^*(m, \mathcal{G}^c(k))$ as $m \to \infty$, where c and k are constants independent of m. Here, we note that members of $\mathcal{G}^c(k)$, as well as extremal hypergraphs for $\mathcal{G}^c(k)$, contain repeated edges. However, in the following, we show that for the purpose of understanding the order of magnitude of $n(m, c, k)$, it is sufficient to restrict our attention on simple hypergraphs only.

Let H be a c-uniform hypergraph that is extremal for the collection $\mathcal{G}^c(k)$. Let H' be a simple c-uniform hypergraph that has maximum number of edges among all simple hypergraphs without having any member of $\mathcal{G}^c(k)$. Then we have the following proposition.

Proposition 3.2. *Let $\mathcal{G}^c(k), H, H'$ be as defined above, then $|H'| \geq \frac{1}{c}|H|$.*

Proof. Since H does not have any member of $\mathcal{G}^c(k)$, an edge of H can have at most c copies. Hence, for the maximal simple sub-hypergraph of H'' of H, it follows that $|H''| \geq \frac{1}{c}|H|$. Now, both H' and H'' are simple hypergraphs without any member of $\mathcal{G}^c(k)$. Hence, from the definition of H', we have that $|H'| \geq |H''| \geq \frac{1}{c}|H|$. □

Now, let

$$\begin{aligned}\mathcal{H}^c(k) =&\{H|H \text{ is a } c\text{-uniform simple hypergraph with } i \text{ edges and } < i \text{ vertices,}\\ &\text{where } 1 \leq i \leq k\} \subseteq \mathcal{G}^c(k).\end{aligned} \tag{3.3}$$

Then, following Proposition 3.2, we have

$$\text{ex}^*(m, \mathcal{G}^c(k)) \leq c\,\text{ex}(m, \mathcal{H}^c(k)). \tag{3.4}$$

Also, since any simple hypergraph not containing any member of $\mathcal{H}^c(k)$ does not contain any member of $\mathcal{G}^c(k)$, we have

$$\text{ex}^*(m, \mathcal{G}^c(k)) \geq \text{ex}(m, \mathcal{H}^c(k)). \tag{3.5}$$

So, from (3.4) and (3.5), we have

$$n(m, c, k) = \text{ex}^*(m, \mathcal{G}^c(k)) = \Theta(\text{ex}(m, \mathcal{H}^c(k))). \tag{3.6}$$

Hence, to understand order of magnitude of $n(m, c, k)$ it is sufficient to consider Turán number of the family $\mathcal{H}^c(k)$ over simple hypergraphs. Furthermore, in the next lemma, we show that the subfamily

$$\begin{aligned}\mathcal{I}^c(k) =&\{H|H \text{ is a simple } c\text{-uniform hypergraph with } i \text{ edges and } i-1 \text{ vertices,}\\ &\text{where } c+3 \leq i \leq k\} \subseteq \mathcal{H}^c(k)\end{aligned} \tag{3.7}$$

can be considered as the forbidden family for our problem at hand. In fact, in Theorem 3.7, where we obtain lower bound on $n(m, c, k)$, we use the subfamily $\mathcal{I}^c(k)$ as the forbidden family.

Lemma 3.3. *Let $\mathcal{H}^c(k)$ and $\mathcal{I}^c(k)$ be defined as above. Then we have*

$$\mathrm{ex}(m, \mathcal{I}^c(k)) = \mathrm{ex}(m, \mathcal{H}^c(k)).$$

Proof. Since $\mathcal{H}^c(k) \supseteq \mathcal{I}^c(k)$, it trivially follows that $\mathrm{ex}(m, \mathcal{H}^c(k)) \leq \mathrm{ex}(m, \mathcal{I}^c(k))$. To prove the other direction, we make the following claim.

***Claim* 3.1.** *Let $H = (\mathcal{V}, \mathcal{F})$ be a simple c-uniform hypergraph such that $|\mathcal{F}| = k$ and $|\mathcal{V}| < k$. Then there is sub-hypergraph (not necessarily an induced one) $H' = (\mathcal{V}', \mathcal{F}')$ of H, such that $|\mathcal{F}'| = \ell$, $|\mathcal{V}'| = \ell - 1$, for some ℓ in the range $c + 2 < \ell \leq k$.*

Proof of the Claim. Indeed, and even in a stronger sense, we can arbitrarily delete edges from H until the condition is satisfied and guaranteed to get the desired sub-hypergraph H'. To show that this always holds, we first observe that any collection of $c + 2$ edges of H spans at least $c + 2$ vertices. So, we have $k > c + 2$. Next, we consider the sequence of sub-hypergraphs $H = H_k \supset H_{k-1} \supset \ldots \supset H_{c+2}$, obtained by arbitrarily deleting edges one by one, where $|H_i| = i$. Let m_i be the number of vertices of H_i for $c + 2 \leq i \leq k$. Then we have $k - m_k \geq 1$, and $c + 2 - m_{c+2} \leq 0$. Now, since $m_i \geq m_{i-1}$ for $c + 3 \leq i \leq k$, we have $(i - m_i) - (i - 1 - m_{i-1}) \leq 1$. Hence, there must be some $H' = H_\ell$, where $c + 2 < \ell \leq k$, such that $\ell - m_\ell = 1$. This proves the claim. □

So, following above claim, any simple hypergraph, that does not contain any member of $\mathcal{I}^c(k)$, does not contain any member of $\mathcal{H}^c(k)$. Hence, $\mathrm{ex}(m, \mathcal{H}^c(k)) \geq \mathrm{ex}(m, \mathcal{I}^c(k))$. So, the lemma follows. □

Following the above discussion, in the sequel, all the considered hypergraphs will be simple unless we state otherwise.

3.1.2 EXISTING RESULTS

Turán type problem, where the forbidden family of is characterized by number of vertices and number edges of the hypergraphs of the family, was introduced by Brown, Erdős, and Sós in [BES73]. There, the authors considered as forbidden family the following family of hypergraphs:

$$\mathcal{H}^c(p, q) = \{H : H \text{ is a } c\text{-uniform hypergraph with } p \text{ vertices and } q \text{ edges }\}. \tag{3.8}$$

They showed, through non-constructive arguments, the following lower bound:

$$\mathrm{ex}(m, \mathcal{H}^c(p,q)) = \Omega(m^{\frac{cq-p}{q-1}}). \tag{3.9}$$

However, the lower bound in (3.9) can not be immediately interpreted as a lower bound on $n(m,c,k)$. In case of (3.9), the forbidden family consists of hypergraphs having a fixed number of vertices and a fixed number of edges. On the other hand, for $n(m,c,k) = \Theta(\mathrm{ex}(m, \mathcal{I}^c(k)))$, we need to consider as forbidden family the hypergraphs whose number of vertices lies within a certain range, and number of edges is one more than the number of vertices.

More recently, a lower bound on $n(m,c,k)$ was obtained in [IKOS04a]. There, the authors obtained the following result using a probabilistic argument:

$$n(m,c,k) = \Omega(m^{c-1}). \tag{3.10}$$

In [PSW09], the authors extended the method of [BES73] for the forbidden family $\mathcal{G}^c(k)$ to obtain the following improvement:

$$n(m,c,k) = \Omega(m^{\frac{kc}{k-1}-1}). \tag{3.11}$$

On the other hand, in [PSW09], the authors showed the following upper bound:

$$n(m,c,k) \leq \frac{(k-1)}{\binom{k-1}{c}}\binom{m}{c}. \tag{3.12}$$

It is trivial to observe that the bound (3.12) is tight for $c = 1$. In [PSW09], it was shown by explicit construction that this bound is also tight for the cases $c = k-1$ and $c = k-2$. Indeed, $k-1$ copies of K_m^{k-1} and a single copy of K_m^{k-2} are the respective constructions.

For our setting of parameters (i.e., for c, k constants independent of m), (3.12) essentially shows that $n(m,c,k) = O(m^c)$. Now, we are considering the Turán number $\mathrm{ex}(m, \mathcal{I}^c(k))$ over simple c-uniform hypergraphs on m vertices. For such hypergraphs there can be at most $\binom{m}{c} = O(m^c)$ edges. Hence, (3.6) and Lemma 3.3 immediately imply $n(m,c,k) = O(m^c)$. Therefore, for our setting of parameters, the upper bound (3.12) is trivial, in terms of order of magnitude.

3.1.3 OUR CONTRIBUTION

Below, we informally list our contributions in this chapter.

(I) We improve the upper bound (3.12) in terms of order of magnitude. In particular, using a result due to Erdős ([Erd64]), we show that $n(m,c,k) = o(m^c)$ for $7 \leq k$, and $3 \leq c \leq k-1-\lceil \log k \rceil$. This result is best possible with respect to the upper bound on c, as we subsequently demonstrate through explicit construction that for $k \geq 6$, and $k - \lceil \log k \rceil \leq c \leq k-1$, $n(m,c,k) = \Theta(m^c)$.

The above mentioned explicit construction improves on the general lower bound, obtained in [PSW09], and also the lower bound (3.9), obtained in [BES73], for the parameters $p = k-1, q = k, k - \lceil \log k \rceil \leq c \leq k-1$, where $k \geq 6$.

(II) For the graph case, i.e., for 2-uniform CBCs, we obtain the following results.

(i) We obtain exact value of $n(m,2,5)$ for $m \geq 5$. We note that exact values of $n(m,2,3)$ and $n(m,2,4)$ are already known due to the bound (3.12) and constructions (corresponding to $c = k-1$ and $c = k-2$ case) given in [PSW09]; namely, we have $n(m,2,3) = m(m-1)$ and $n(m,2,4) = \binom{m}{2}$.

(ii) Using a result (regarding maximum size of graphs with large girth) of Lazebnik *et al.* [LUW95], we improve the existing lower bound $n(m,2,k) = \Omega(m^{\frac{k+1}{k-1}})$, obtained in [PSW09], for all $k \geq 8$ and infinitely many values of m.

(iii) We show $n(m,2,k) = O(m^{1+\frac{1}{\lfloor \frac{k}{4} \rfloor}})$ using a result due to Bondy and Simonovits [BS74].

(iv) For small values of k, we obtain the following exact orders of magnitude:

(a) $n(m,2,k) = \Theta(m^{\frac{3}{2}})$ for $k = 6,7,8$;

(b) $n(m,2,k) = \Theta(m^{\frac{4}{3}})$ for $k = 9,10,11$;

(c) $n(m,2,k) = \Theta(m^{\frac{6}{5}})$ for $k = 15,16,17$.

(III) In Section 3.2.3, we briefly discuss Turán density of the family $\mathcal{I}^3(6)$. For 3-uniform CBCs, Theorem 3.7 indicates $n(m,3,k) = \theta(m^3)$ for $k \leq 6$. So, we have positive Turán density for families $\mathcal{I}^3(k)$, for $k \leq 6$. Hence, it is meaningful to investigate Turán densities of these families. Now, we observe that $\text{ex}(m,\mathcal{I}^3(4)) = \text{ex}(m,\mathcal{I}^3(5)) = \binom{m}{3}$ (indeed, it is trivial to see that both are $\leq \binom{m}{3}$, and in both the cases K_m^3 is the extremal graph). Hence, we have

$$\pi(\mathcal{I}^3(4)) = \lim_{m\to\infty} \frac{\text{ex}(m,\mathcal{I}^3(4))}{\binom{m}{3}} = 1,$$

and

$$\pi(\mathcal{I}^3(5)) = \lim_{m\to\infty} \frac{\text{ex}(m,\mathcal{I}^3(5))}{\binom{m}{3}} = 1.$$

However, the case of $\pi(\mathcal{I}^3(6))$ is much involved, and we only have partial answer for it. We relate Turán density of $\mathcal{I}^3(6)$ to much studied Turán density of K_4^{3-} (in this case, the forbidden family consists of the single member K_4^{3-}), where K_4^{3-} is the 3-uniform hypergraph on 4 vertices with 3 edges . In fact, we essentially show that Turán densities of the two families are same. Hence, existing upper and lower bounds on Turán density of K_4^{3-} apply for the family $\mathcal{I}^3(6)$ as well.

3.2 Results and Proofs

3.2.1 c-uniform case for $c \geq 3$

We begin this section by stating the following result due to Erdős that will be crucial in our proof of Theorem 3.5.

Theorem 3.4 ([Erd64]). *Let m, c, ℓ be positive integers, with $\ell > 1$ and $m > m_0(c,\ell)$, where $m_0(c,\ell)$ is an integer that depends only on c and ℓ. Then for sufficiently large C, where C is independent of m, c, and ℓ, we have*

$$m^{c-\frac{C}{\ell^{c-1}}} < \text{ex}(m, K^c(\ell,\ldots,\ell)) \leq m^{c-\frac{1}{\ell^{c-1}}}.$$

Now, we show that $n(m,c,k) = o(m^c)$ for $7 \leq k$, and $3 \leq c \leq k-1-\lceil \log k \rceil$. All the logarithms mentioned in this chapter are to the base 2.

Theorem 3.5. *Let $k \geq 7$, and $3 \leq c \leq k - 1 - \lceil \log k \rceil$. Then for sufficiently large m ($m > m_1(c)$, where m_1 is a constant that depends only on c), $n(m, c, k) \leq cm^{c - \frac{1}{2^{c-1}}}$.*

Proof. Let u, v be such that $7 \leq u \leq k, 1 \leq v \leq u - 2\lceil \log u \rceil$, and $c = u - v - \lceil \log u \rceil$. It is possible to find such u, v for the range of values of c stated in the theorem. Next, we consider the c-uniform, complete c-partite hypergraph $\mathcal{H} = (\mathcal{V}, \mathcal{F})$, where

$$\mathcal{V} := \{x_1, \ldots, x_{u-v-2\lceil \log u \rceil}, \ldots, x_c, y_1, \ldots, y_{u-v-2\lceil \log u \rceil}, \ldots, y_c\}$$

and

$$\mathcal{F} := \Big\{\{z_1, \ldots, z_c\} : z_i \in \{x_i, y_i\}, 1 \leq i \leq c\Big\}.$$

Now, we apply Theorem 3.4 with $\mathcal{H} = K^{(c)}(2, \ldots, 2)$. We get, for sufficiently large m, i.e., for $m > m_0(c, 2) = m_1(c)$

$$\mathrm{ex}(m, \mathcal{H}) \leq m^{c - \frac{1}{2^{c-1}}}. \tag{3.13}$$

Next, we consider the c-uniform sub-hypergraph $\mathcal{H}' = (\mathcal{V}', \mathcal{F}')$ of $\mathcal{H}$, where

$$\mathcal{V} \supseteq \mathcal{V}' := \{x_1, \ldots, x_{u-v-2\lceil \log u \rceil}, \ldots, x_c, y_{u-v-2\lceil \log u \rceil+1}, \ldots, y_c\}$$

and

$$\mathcal{F}' := \Big\{\{x_1, \ldots, x_{u-v-2\lceil \log u \rceil}, z_{u-v-2\lceil \log u \rceil+1}, \ldots, z_c\} : z_j \in \{x_j, y_j\}, \\ u - v - 2\lceil \log u \rceil + 1 \leq j \leq c\Big\}.$$

Since $v \geq 1$, we have

$$|\mathcal{V}'| = u - v \leq u - 1, \tag{3.14}$$

and

$$|\mathcal{F}'| = 2^{\lceil \log u \rceil} \geq u. \tag{3.15}$$

Now, since $u \leq k$, $\mathcal{H}' \in \mathcal{H}^c(k)$, where $\mathcal{H}^c(k)$ is the family defined in (3.3). So, we have

$$\mathrm{ex}(m, \mathcal{H}^c(k)) \leq \mathrm{ex}(m, \mathcal{H}') \leq \mathrm{ex}(m, \mathcal{H}).$$

Hence, from (3.4) and (4.9), we get for sufficiently large m, i.e., for $m > m_1(c)$,

$$n(m,c,k) \leq cm^{c-\frac{1}{2^c-1}}. \qquad \square$$

In the following example, we demonstrate the construction of the forbidden hypergraph for small parameter values.

Example 3.1. Let $c = 4, k = 8$. We choose $u = 8$, which yields $v = u - \lceil \log u \rceil - c = 1$. So, $\mathcal{H} = (\mathcal{V}, \mathcal{F})$, where $\mathcal{V} = \{x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4\}$ and $\mathcal{F} = \{x_1, y_1\} \times \{x_2, y_2\} \times \{x_3, y_3\} \times \{x_4, y_4\}$. Similarly, as forbidden hypergraph we can consider $\mathcal{H}' = (\mathcal{V}', \mathcal{F}') \subset \mathcal{H}$, where $\mathcal{V}' = \{x_1, x_2, x_3, x_4, y_2, y_3, y_4\}$, and $\mathcal{F}' = \{x_1\} \times \{x_2, y_2\} \times \{x_3, y_3\} \times \{x_4, y_4\}$. Consequently, $7 = |\mathcal{V}'| \leq |\mathcal{F}'| = 8$.

A few remarks regarding the theorem are in order.

Remark 3.6.

1. Each edge of $\mathcal{F}'$ has the fixed set of vertices $\{x_1, \ldots, x_{u-v-2\lceil \log u \rceil}\}$. This choice is arbitrary. Any fixed set of $u - v - 2\lceil \log u \rceil$ vertices $\{z_1, \ldots, z_{u-v-2\lceil \log u \rceil}\}$ can be selected subject to the condition $z_j \in \{x_j, y_j\}$, where $1 \leq j \leq u - v - 2\lceil \log u \rceil$.

2. We also observe that the same construction with partite sets of size ℓ, along with Theorem 3.4, produces similar result for $c \leq k - 1 - (\ell - 1)\lceil \log_\ell k \rceil$.

3. Inequalities (3.14) and (3.15) are tight when u is a power of 2 and $v = 1$. In particular, when k is a power of 2 and $c = k - 1 - \log k$, we have $|\mathcal{V}'| = k - 1$ and $|\mathcal{F}'| = k$. So, k edges of $\mathcal{H}'$ span exactly $k - 1$ vertices.

In the next theorem, we show that the bound $c \leq k - \lceil \log k \rceil - 1$, in Theorem 3.5, is tight. More precisely, our result is the following.

Theorem 3.7. *$n(m,c,k) = \Theta(m^c)$ for $6 \leq k$, $k - \lceil \log k \rceil \leq c \leq k - 1$.*

Proof. Here, we show that $n(m,c,k) = \Omega(m^c)$ for the stated ranges of values of c and k. This, together with $n(m,c,k) = O(m^c)$ from (3.12), would imply $n(m,c,k) = \Theta(m^c)$. First, we prove the above for $c = k - \lceil \log k \rceil$, as this turns out to be the tight case. The same argument holds for the rest of the range of values of c. Note that the cases $c = k - 1$ and $c = k - 2$ have already been settled in [PSW09].

Construction: Let $\mathcal{H} = (\mathcal{V}, \mathcal{F})$ be a complete c-uniform, c-partite hypergraph, where $\mathcal{V} = \mathcal{V}_1 \cup \mathcal{V}_2 \cup \ldots \cup \mathcal{V}_c$, such that $\mathcal{V}_i \cap \mathcal{V}_j = \emptyset$ for $i \neq j$, and $|\mathcal{V}_i| = \lfloor \frac{m+i-1}{c} \rfloor$ for $1 \leq i \leq c$. Clearly, $|\mathcal{F}| = \Omega(m^c)$.

In the following claim, we show that $\mathcal{H}$ does not contain any member of $\mathcal{I}_c(k)$, where $\mathcal{I}_c(k)$ is as defined in (3.7). This, together with Lemma 3.3 and (3.5), implies $n(m, c, k) = \Omega(m^c)$.

***Claim* 3.2.** *$\mathcal{H}$ does not contain a sub-hypergraph $\mathcal{H}' = (\mathcal{V}', \mathcal{F}')$ such that $|\mathcal{V}'| = i-1$ and $|\mathcal{F}'| \geq i$ for $c+3 \leq i \leq k$.*

Proof. First, we observe that if there is a sub-hypergraph $\mathcal{H}' = (\mathcal{V}', \mathcal{F}')$ such that $|\mathcal{V}'| = i - 1$ and $|\mathcal{F}'| \geq i$ for some $c + 3 \leq i < k$, then there is another sub-hypergraph $\mathcal{H}'' = (\mathcal{V}'', \mathcal{F}'')$ such that $\mathcal{H}' \subseteq \mathcal{H}'' \subseteq \mathcal{H}$, $|\mathcal{V}''| = k-1$, and $|\mathcal{F}''| \geq k$. To get $\mathcal{H}''$ from $\mathcal{H}'$ we add $k - i$ edges to $\mathcal{F}'$ with the following condition. Each of the added $k - i$ edges contains exactly one unique vertex not contained in $\mathcal{V}'$, i.e., there are newly added $k - i$ vertices, each belonging to a unique newly added edge. This is always possible due to the structure of $\mathcal{H}$, provided there are $k - i$ distinct vertices in $\mathcal{V} \setminus \mathcal{V}'$. But this can be safely assumed because m is large enough; in fact, $m \geq k$ is sufficient. Hence, it is sufficient to establish that $\mathcal{H}$ does not contain a sub-hypergraph $\mathcal{H}' = (\mathcal{V}', \mathcal{F}')$ such that $|\mathcal{V}'| = k - 1$ and $|\mathcal{F}'| \geq k$. In other words, we need to show that any subset of $\mathcal{V}$ of size $k - 1$ spans at most $k - 1$ edges.

Let $\mathcal{V}' \subseteq \mathcal{V}$, with $|\mathcal{V}'| = k - 1$. So, $\mathcal{V}' = \mathcal{V}'_1 \cup \mathcal{V}'_2 \cup \ldots \cup \mathcal{V}'_c$, where $\mathcal{V}'_i \subseteq \mathcal{V}_i$ for $1 \leq i \leq c$. Furthermore, we note that $|\mathcal{V}'_i| \geq 1$ for each i; otherwise, $\mathcal{F}'$ is empty. Now, we have

$$\sum_{i=1}^{c} |\mathcal{V}'_i| = |\mathcal{V}'| = k - 1, \text{ and } |\mathcal{F}'| = \prod_{i=1}^{c} |\mathcal{V}'_i|. \tag{3.16}$$

Next, we observe that subject to (3.16), $|\mathcal{F}'|$ attains its maximum when $|\mathcal{V}'_i|$s are as equal as possible, i.e., when

$$||\mathcal{V}'_i| - |\mathcal{V}'_j|| \leq 1, \text{ for } 1 \leq i, j \leq c. \tag{3.17}$$

We show this by the following argument. First, let us assume, without loss of generality, that $|\mathcal{V}'_2| - |\mathcal{V}'_1| \geq 2$ when $|\mathcal{F}'|$ attains its maximum value; we denote this maximum by F_{max}. So, let $|\mathcal{V}'_1| = r$, $|\mathcal{V}'_2| = r + \ell$, where $r \geq 1$ and $\ell \geq 2$.

Remaining $|\mathcal{V}_i^{'}|$s, i.e., $|\mathcal{V}_i^{'}|$s for $3 \leq i \leq c$, have arbitrary but fixed values. So, we have $F_{max} = \prod_{i=1}^{c}|\mathcal{V}_i^{'}| = (r^2 + r\ell)\prod_{i=3}^{c}|\mathcal{V}_i^{'}|$. Next, we modify $|\mathcal{V}_1^{'}|$ and $|\mathcal{V}_2^{'}|$ keeping the other $|\mathcal{V}_i^{'}|$s same. Let $|\mathcal{V}_1^{'}| = r+1, |\mathcal{V}_2^{'}| = r+\ell-1$. So, clearly $\sum_{i=1}^{c}|\mathcal{V}_i^{'}| = k-1$. However, in this case we have $|\mathcal{F}^{'}| = \prod_{i=1}^{c}|\mathcal{V}_i^{'}| = (r^2+\ell r+\ell-1)\prod_{i=3}^{c}|\mathcal{V}_i^{'}| > F_{max}$ for $\ell \geq 2$. This contradicts the fact that maximum value of $|\mathcal{F}^{'}|$ is F_{max}.

Here, we note that $|\{\mathcal{V}_i^{'} : |\mathcal{V}_i^{'}| = 1, 1 \leq i \leq c\}| \geq 2c-k+1 \geq 1$ for $6 \leq k$, and $c = k - \lceil \log k \rceil$; otherwise, we have $\sum_{i=1}^{c}|\mathcal{V}_i^{'}| > k-1$, a contradiction. Hence, from (3.17), it follows that when $|\mathcal{F}^{'}|$ is maximum we have $|\mathcal{V}_i^{'}| \in \{1,2\}$ for $1 \leq i \leq c$. But this implies that, in this case, there are exactly $(k-c-1)$ $\mathcal{V}_i^{'}$s, $1 \leq i \leq c$ with $|\mathcal{V}_i^{'}| = 2$, and for the remaining $2c-k+1$ $\mathcal{V}_i^{'}$s, $|\mathcal{V}_i^{'}| = 1$.

So, finally we have

$$|\mathcal{F}^{'}| \leq 2^{k-c-1} = 2^{\lceil \log k \rceil - 1} \leq k-1.$$

Hence, the claim is proven. □

Now, repeating the same argument as above for the cases with c in the range $k - \lceil \log k \rceil < c \leq k-1$, we observe that $|\mathcal{F}^{'}| \leq 2^{k-c-1} < 2^{\lceil \log k \rceil - 1} \leq k-1$. Hence, the theorem. □

3.2.2 2-UNIFORM CASE

For 2−uniform (graph) CBCs, we obtain the following improvements over existing results.

3.2.2.1 AN EXACT RESULT

As we have discussed in Section 3.1.3, exact values of $n(m,2,k)$ are already known for $k = 3,4$. In the following theorem, we obtain the exact value of $n(m,2,5)$.

Theorem 3.8. *$n(m,2,5) = \lfloor \frac{m^2}{4} \rfloor$ for $m \geq 5$.*

Proof. In [PSW09], the authors observed that $n(m,2,5) \geq \lfloor \frac{m^2}{4} \rfloor$. Indeed, a complete bipartite graph on $m (m \geq 5)$ vertices with partite sets having $\lceil \frac{m}{2} \rceil$ and

$\lfloor \frac{m}{2} \rfloor$ vertices is a 2-uniform CBC with $k = 5$ and $n = \lfloor \frac{m^2}{4} \rfloor$. Hence, it suffices to prove that $n(m, 2, 5) \leq \lfloor \frac{m^2}{4} \rfloor$. This is an exact result. So, here we need to show that $n(m, 2, 5) = \text{ex}^*(m, \mathcal{G}_2(5)) \leq \lfloor \frac{m^2}{4} \rfloor$, where $\mathcal{G}_2(5)$ is the forbidden family of multigraphs (i.e., graphs with repeated edges) defined according to (3.2).

We show that any multigraph with m vertices and at least $\lfloor \frac{m^2}{4} \rfloor + 1$ edges contains a sub-multigraph with 4 vertices and 5 edges. We prove this by induction on m. This is clearly true for $m = 4$. Now, suppose we have a multigraph with m vertices and at least $\lfloor \frac{m^2}{4} \rfloor + 1$ edges. In fact, we assume that the multigraph has exactly $\lfloor \frac{m^2}{4} \rfloor + 1$ edges by removing any extra edges from the given multigraph. We observe that the multigraph contains a vertex of degree at most $\lfloor \frac{m}{2} \rfloor$. Removing this vertex along with all its incident edges leaves a multigraph with $m - 1$ vertices and at least $\lfloor \frac{(m-1)^2}{4} \rfloor + 1$ edges. By the induction hypothesis, the resulting multigraph contains a sub-multigraph with 4 vertices and 5 edges. □

3.2.2.2 IMPROVEMENT OF THE LOWER BOUND

The lower bound (3.11), obtained in [PSW09], implies $n(m, 2, k) = \Omega(m^{\frac{k+1}{k-1}})$. Here, we improve this lower bound on $n(m, 2, k)$ for all k and infinitely many values of m. We need the following lemma, which also appears as an exercise in [Bol98]. For the sake of completeness, we include its proof.

Lemma 3.9. *Let $k \geq 6$. If a graph has k edges and at most $k - 1$ vertices then it has girth at most $\lfloor \frac{2k}{3} \rfloor$. This bound is tight.*

Proof. The statement is true for $k = 6$. Let us assume that the statement does not hold for some $k > 6$. We choose k minimum so that the statement does not hold, i.e., for this minimum k we have a graph G with k edges, at most $k - 1$ vertices, and the girth of G is $\geq \lfloor \frac{2k}{3} \rfloor + 1$. Without loss of generality, we assume that the graph is connected. Since G has k edges and at most $k - 1$ vertices, it contains at least 2 distinct cycles. Let the cycles be C_1, C_2. Now, if C_1 and C_2 are edge disjoint then one of them will have length at most $\lfloor \frac{k}{2} \rfloor < \lfloor \frac{2k}{3} \rfloor$ which contradicts the assumption on the girth of G.

Let $E(C_i)$ be the set of edges of C_i for $i \in \{1, 2\}$. If C_1 and C_2 are not edge disjoint, let $\ell_0 = |E(C_1) \cap E(C_2)|$ be the number of common edges between C_1 and C_2.

Also, let ℓ_1 and ℓ_2 be the number of edges that exclusively belong to C_1 and C_2 respectively. So, by the assumption on the girth of G we have

$$\ell_0 + \ell_1 = |E(C_1)| \geq \lfloor \frac{2k}{3} \rfloor + 1, \text{ and } \ell_0 + \ell_2 = |E(C_2)| \geq \lfloor \frac{2k}{3} \rfloor + 1. \tag{3.18}$$

Now, we consider the subgraph of G consisting of the edges of $E(C_1) \Delta E(C_2)$, where Δ refers to the symmetric difference of the corresponding edge sets. It follows that every vertex in this subgraph has even degree. So, it contains a cycle. Again, by the assumption on the girth of G we have

$$\ell_1 + \ell_2 \geq \lfloor \frac{2k}{3} \rfloor + 1. \tag{3.19}$$

From (3.18) and (3.19) we have $\ell_0 + \ell_1 + \ell_2 > k$, a contradiction.

This bound is tight as shown by a *theta graph*[5] $\theta(3, \frac{k}{3})$ (for k a multiple of 3). $\theta(3, \frac{k}{3})$ has $k-1$ vertices, k edges, and girth $\frac{2k}{3}$. □

Our improvement on the lower bound on $n(m, 2, k)$, stated as Corollary 3.11, is a consequence of the following result of [LUW95].

Theorem 3.10 ([LUW95]). *For $s \geq 2$, $\text{ex}(m, \{C_3, C_4, \ldots, C_{2s+1}\}) = \Omega(m^{1+\frac{2}{3s-3+\varepsilon}})$ for infinitely many values of m, where $\varepsilon = 0$ if s is odd, and $= 1$ if s is even.*

Informally, Theorem 3.10 provides a (explicit) construction of a graph with "many" edges that does not contain "small" cycles. Lemma 3.9 implies that such a graph is a 2-uniform CBC with large n. More specifically, our result is the following.

Corollary 3.11. *Let $k \geq 8$, then*

$$n(m, 2, k) = \begin{cases} \Omega(m^{\frac{k-3}{k-5}}) & \text{if } k = 5 \mod 6 \\ \Omega(m^{\frac{k-2}{k-4}}) & \text{if } k = 2 \mod 6 \text{ or } k = 4 \mod 6 \\ \Omega(m^{\frac{k-1}{k-3}}) & \text{if } k = 1 \mod 6 \text{ or } k = 3 \mod 6 \\ \Omega(m^{\frac{k}{k-2}}) & \text{if } k = 0 \mod 6 \end{cases}$$

for infinitely many values of m.

Proof. The proof follows directly from Lemma 3.9 and Theorem 3.10. □

[5] Given integers t and ℓ, the theta graph $\theta(t, \ell)$ is a graph on $t\ell - t + 2$ vertices and $t\ell$ edges such that two particular vertices are joined by t vertex disjoint paths of length ℓ. By setting $T = K_{1,t}$, and connecting the t vertices of one partition with a vertex outside of T by t vertex disjoint paths of length $\ell - 1$ we get $\theta(t, \ell)$.

Remark 3.12.

1. For the cases where $k = 0 \mod 3$ or $k = 1 \mod 3$, the bounds of the Corollary 3.11 may be improved. Lemma 3.9 requires the girth to be $\lfloor \frac{2k}{3} \rfloor + 1$, which is odd in these cases. Whereas, the bounds for these cases were obtained by applying Theorem 3.10 for graphs of girth $\lfloor \frac{2k}{3} \rfloor + 2$.

2. The lower bound (3.11) is probabilistic, i.e., non-constructive. On the other hand, the construction of Theorem 3.10 is strongly explicit (we will discuss this notion in detail in Chapter 4). This, in turn, means the construction of CBCs in Corollary 3.11 is also strongly explicit. Strongly explicit constructions are very useful for practical applications.

3.2.2.3 IMPROVEMENT OF THE UPPER BOUND

The upper bound $n(m, c, k) \leq cm^{c-\frac{1}{2^{c-1}}}$, that we have obtained in Theorem 3.5, implies $n(m, 2, k) = O(m^{\frac{3}{2}})$. Here, we improve this upper bound on $n(m, 2, k)$. The next theorem from [BS74] is crucial for our proof.

Theorem 3.13. *([BS74]) If in a graph of order m, the number of edges $> 100km^{1+\frac{1}{k}}$, then the graph contains a $C_{2\ell}$ for every $\ell \in [k, km^{\frac{1}{k}}]$.*

Informally, Theorem 3.13 shows that a graph with "many" edges has a "small" cycle. There have been improvements (cf. [Ver00], [Pik12]) in the constant term ($100k$) of this important theorem. However, our focus is on the order of magnitude of the upper bound, and we do not require best of the constants for our result. So, we use Theorem 3.13. We utilize this to show that such a graph can not be a 2-uniform CBC. In particular, our result is the following.

Theorem 3.14. *For $k \geq 4$, $n(m, 2, k) = O(m^{1+\beta})$, where $\beta = \frac{1}{\lfloor \frac{k}{4} \rfloor}$.*

In the proof of Theorem 3.14, we need the following observation. This is a folklore result in this area. We include its proof for the sake of completeness.

Observation 3.1. *In any finite graph G, there is a non-empty subgraph H with the following properties. Minimum vertex degree of H is at least one fourth of the average vertex degree of G, and size of H is at least half of the size of G.*

Proof. Let the number of vertices and the average degree of vertices of G be m and d_{avg} respectively. Therefore, the number of edges of G is given by $\frac{md_{avg}}{2}$.

Next, we delete vertices of G having degree less than $\frac{d_{avg}}{4}$ one by one. Since there are only finitely many vertices in G, we terminate after finitely many steps with a subgraph H. Now, to show that H is non-empty it is sufficient to show that the average degree of vertices increases after each step. Indeed, at the end of the first step, the number of edges in the resulting graph is $\geq \frac{md_{avg}}{2} - \frac{d_{avg}}{4}$. Hence, at the end of first step average degree of vertices is $> d_{avg}$. Similar argument holds for subsequent steps. Next, total number of edges deleted before termination is at most $\frac{md_{avg}}{4}$. Hence, number of edges in H is at least $\frac{md_{avg}}{4}$. □

Proof of Theorem 3.14. Here we show that $n(m, 2, k) \leq 200km^{1+\beta}$. Let G be a graph with $200km^{1+\beta}$ edges. Hence, by Observation 3.1, G has a subgraph H with at least $100km^{1+\beta}$ edges and minimum vertex degree at least $100km^{\beta}$. So, Theorem 3.13 implies that H has a cycle C of length at most $2\lfloor\frac{k}{4}\rfloor$. Let $v \in C$ be an arbitrary vertex. We consider all the walks of length $\lfloor\frac{k}{4}\rfloor$ in H starting at v such that no edge of H repeats consecutively in any of the walks. Clearly, the number of such walks is

$$100km^{\beta}(100km^{\beta} - 1)^{\lfloor\frac{k}{4}\rfloor - 1} > m.$$

Consequently, there is a vertex v' such that at least two distinct walks of length $\lfloor\frac{k}{4}\rfloor$ starting at v terminate at v'. These two walks along with C constitute a subgraph of H with ℓ edges spanning at most $\ell - 1$ vertices, where $\ell \leq k$. Hence, G is not a CBC. □

3.2.2.4 EXACT ORDERS OF MAGNITUDE

From earlier results ([PSW09] and Theorem 3.8), exact values of $n(m, 2, k)$ are known for $k = 3, 4, 5$. Here, we derive exact orders of magnitude of $n(m, 2, k)$ for subsequent specific values of k. Below, we list these cases.

(*i*) Theorem 3.14 implies trivial upper bound $O(m^2)$ on $n(m, 2, k)$ for $k = 6, 7$. We improve on this trivial upper bound on $n(m, 2, k)$ for $k = 6, 7$, by the following well-known theorem due to Kővári *et al.*

Theorem 3.15 ([KST54], see also [Bol78]). *Suppose* $2 \leq s$, $2 \leq t$, *and* $s \geq t$. *Then* $\mathrm{ex}(m, K(s, t)) \leq \frac{1}{2}(s-1)^{\frac{1}{t}}(m - t + 1)m^{1-\frac{1}{t}} + \frac{1}{2}(t-1)m$.

Corollary 3.16. $n(m, 2, k) = \Theta(m^{\frac{3}{2}})$ *for* $k = 6, 7, 8$.

Proof. Theorem 3.15 clearly implies $\text{ex}(m, K(s,2)) = O(m^{\frac{3}{2}})$. More precisely, it implies that there is a constant $c_{s,2}$ such that for all sufficiently large m, any graph of order m with more than $c_{s,2}m^{\frac{3}{2}}$ edges contains a $K(s,2)$. Next, we consider $K(\lceil \frac{k}{2} \rceil, 2)$. It has $\geq k$ edges and $\leq k-1$ vertices for $k \geq 6$. Hence, it has a subgraph where k edges span $\leq k-1$ vertices. This implies $n(m,2,k) \leq \text{ex}(m, K(\lceil \frac{k}{2} \rceil, 2)) = O(m^{\frac{3}{2}})$ for $k \geq 6$.

Now, we show tightness of the above mentioned upper bound for the cases $k = 6, 7, 8$. We note that Lemma 3.9 implies that a graph which is $\{C_3, C_4, C_5\}$-free, is a 2-uniform CBC with $k \leq 8$. Now, it is well-known (cf. [Bol78]) that for q a prime power, the incidence graph of $PG(2,q)$ is a $(q+1)$-regular bipartite graph with $2(q^2+q+1)$ vertices and girth 6. In fact, and it was shown in [ERS66], for sufficiently large m (and not just when $m = 2(q^2+q+1)$ for a prime power q) this construction leads to a graph on m vertices having $\Omega(m^{\frac{3}{2}})$ edges whose girth is 6. [6] So, finally we have $n(m,2,k) = \Omega(m^{\frac{3}{2}})$ for $k = 6, 7, 8$. □

In the following two cases, uppper bound on the order of magnitude of $n(m,2,k)$ follows from a recent result of [BT15]. There, the authors have shown $n(m,2,k) = O(m^{1+\frac{1}{\lfloor \frac{k}{3} \rfloor}})$. This is an improvement on the upper bound, obtained in Theorem 3.14. We will briefly discuss the results of [BT15] in Section 3.3.

(*ii*) $n(m,2,k) = \Theta(m^{\frac{4}{3}})$, for $k = 9, 10, 11$. In this case, the lower bound on the order of magnitude follows from Corollary 3.11.

(*iii*) $n(m,2,k) = \Theta(m^{\frac{6}{5}})$, for $k = 15, 16, 17$. In this case, the lower bound on the order of magnitude follows by considering the incidence graph of finite generalized hexagon (cf. [PT09]) of order q, where q is a prime power. The graph is a $(q+1)$-regular bipartite graph of girth 12 and has partite sets of size $q^5+q^4+q^3+q^2+q+1$. This, together with Lemma 3.9 and a consideration similar to [ERS66], discussed for (*i*) above, implies the result.

3.2.3 TURÁN DENSITY OF $\mathcal{I}^3(6)$

Our main theorem in this section is the following.

[6] This construction also improves on the non-constructive lower bound in (3.11) for $n(m,2,7)$ and $n(m,2,8)$.

Theorem 3.17. $\pi(\mathcal{I}^3(6)) = \pi(K_4^{3-})$, *where* K_4^{3-} *is the* 3*-uniform hypergraph on* 4 *vertices with* 3 *edges.*

Now, from the bounds on $\pi(K_4^{3-})$, we have the following upper and lower bounds on the Turán density of the family $\mathcal{I}^3(6)$.

Corollary 3.18. $\frac{2}{7}(1 - o(1)) \leq \pi(\mathcal{I}^3(6)) \leq 0.2871$

In [Cae83], it was shown that $\pi(K_4^{3-}) \leq \frac{1}{3}$. This was subsequently improved in [Mub03, MT08, Raz10, Tal07]. The present upper bound (0.2871) was obtained in [BT11], using *flag algebras* (cf. [Raz07]), and the lower bound was obtained in [FF84]. Here, we will not discuss flag algebras because the topic is much advanced and involved. However, we find it motivating to discuss the construction from [FF84] that leads to the lower bound in Corollary 3.18. We will discuss it after the proof of Theorem 3.17. To prove Theorem 3.17 we need the idea of *blow-up* (see [Kee11] for further details).

Let H be a c-uniform hypergraph. t-blow-up of H, denoted as $H(t)$, is obtained in the following manner. Each vertex v of H is replaced by t copies $v^1, v^2, \ldots, v^t$ in $H(t)$. Each edge of H is replaced by a copy of a c-partite c-uniform hypergraph on the blown-up vertices of the edge. More precisely, an edge $\{v_1, v_2, \ldots, v_c\}$ of H is replaced in $H(t)$ with a c-partite c-uniform hypergraph $\left\{\{v_1^{w_1}, v_2^{w_2}, \ldots, v_c^{w_c}\} | 1 \leq w_i \leq t, 1 \leq i \leq c\right\}$. The next theorem, which is implied by a result of [Erd71], states that Turán densities of a hypergraph and its t-blowup are the same. We need this in our proof of Theorem 3.17.

Theorem 3.19 (cf. [Kee11])**.** $\pi(H) = \pi(H(t))$ *for constant* t*.*

Proof of Theorem 3.17: First, we show $\pi(K_4^{3-}) \leq \pi(\mathcal{I}^3(6))$. Consider a hypergraph H^3 having $\text{ex}(m, \mathcal{I}_3(6)) + 1$ edges. So, there is $H'^3 = \{\mathcal{V}', \mathcal{E}'\} \subseteq H^3$, with $|\mathcal{V}'| = 5, |\mathcal{E}'| = 6$. Next, we observe that there is $v \in \mathcal{V}'$, such that $deg_{H'^3}(v) \leq 3$; otherwise, $\sum_{v \in \mathcal{V}'} deg_{H'^3}(v) \geq 20 > 18 = \sum_{e \in \mathcal{E}'} |e|$, a contradiction. By removing v and its incident edges from H'^3 we get a set of 4 vertices that span at least 3 edges. So, $\text{ex}(m, K_4^{3-}) \leq \text{ex}(m, \mathcal{I}^3(6))$.

Now, we show $\pi(K_4^{3-}) \geq \pi(\mathcal{I}^3(6))$ [7]. Let $K_4^{3-} = \{\mathcal{V}, \mathcal{E}\}$, where $\mathcal{V} = \{v_1, v_2, v_3, v_4\}$, and $\mathcal{E} = \{\{v_1, v_2, v_3\}, \{v_1, v_2, v_4\}, \{v_1, v_3, v_4\}\}$, without loss of generality.

[7] This part was proven by Dhruv Mubayi [Mub12].

Next, we consider a hypergraph H^3 with $(\pi(K_4^{3-}) + \varepsilon)\binom{m}{3}$ edges, where $\varepsilon > 0$. So, according to Theorem 3.19, there is a sub-hypergraph $H'^3 = \{\mathcal{V}', \mathcal{E}'\} \subseteq H^3$ which is a 2-blowup of K_4^{3-}. Let $\mathcal{V}' = \{v_1^1, v_1^2, v_2^1, v_2^2, v_3^1, v_3^2, v_4^1, v_4^2\}$. In K_4^{3-}, the vertex v_1 has degree 3. We exploit this to construct two copies of K_4^{3-} in H'^3. In place of v_1, these two copies of K_4^{3-} have its (blown-up) copies v_1^1, v_1^2 respectively. More precisely, in the blow-up of K_4^{3-} there is the sub-hypergraph consisting of the 6 edges - $\{v_1^1, v_2^1, v_3^1\}, \{v_1^1, v_2^1, v_4^1\}, \{v_1^1, v_3^1, v_4^1\}, \{v_1^2, v_2^1, v_3^1\}, \{v_1^2, v_2^1, v_4^1\}, \{v_1^2, v_3^1, v_4^1\}$, on the 5 vertices $\{v_1^1, v_2^1, v_3^1, v_4^1, v_1^2\}$. This sub-hypergraph is a member of $\mathcal{I}_3(6)$. Hence, $\pi(K_4^{3-}) \geq \pi(\mathcal{I}^3(6))$. □

Construction showing $\pi(K_4^{3-}) \geq \frac{2}{7}(1 - o(1))$ *[FF84].* Let $H = (\mathcal{V}, \mathcal{E})$, where $|\mathcal{V}| = m$. We partition $\mathcal{V}$ as $\mathcal{V} = \mathcal{V}_1 \bigcup \cdots \bigcup \mathcal{V}_6$, where $|\mathcal{V}_i| \in \{\left\lfloor \frac{m}{6} \right\rfloor, \left\lceil \frac{m}{6} \right\rceil\}, 1 \leq i \leq 6$. To define the edge set let us define the set $S_6 = \{\{1,2,3\}, \{1,2,4\}, \{1,3,5\}, \{1,4,6\}, \{1,5,6\}, \{3,4,5\}, \{3,4,6\}, \{2,3,6\}, \{2,5,6\}, \{2,4,5\}\}$. On the left of Figure 3.1, we present a pictorial view of the set (as was done in [FF84]).

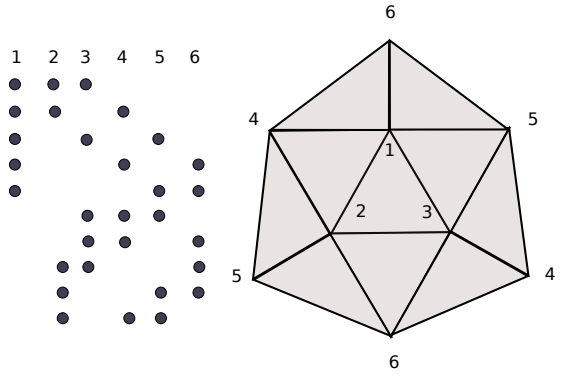

FIGURE 3.1: S_6

In fact, elements of S_6 are given by the triangles of graph, given on the right of Figure 3.1. Vertices of each triangle constitute an element of S_6. we note that, in the graph, any four of the six points $\{1,2,3,4,5,6\}$ span either 0 or 2 triangles.

Next, we take the edge set to be the set $\{\{x,y,z\} | x \in \mathcal{V}_i, y \in \mathcal{V}_j, z \in \mathcal{V}_k, \{i,j,k\} \in S_6\}$, along with the edges generated by applying the same construction recursively on each $\mathcal{V}_i, 1 \leq i \leq 6$. So,

$$|\mathcal{E}| = 10\left(\frac{m}{6}\right)^3 \left\{1 + \left(\frac{1}{6}\right)^2 + \left(\frac{1}{6}\right)^4 + \cdots\right\} \approx \frac{m^3}{21}(1 - o(1)).$$

From the construction, we observe that any set of 4 vertices either spans no edge or exactly 2 edges. So, $\pi(K_4^{3-}) \geq \frac{2}{7}(1 - o(1))$.

3.3 CONCLUDING REMARKS

In a very recent work ([BT15]), the authors have improved the upper bound on $n(m, c, k)$ further. They consider the following family of forbidden hypergraphs:

$$\mathcal{J}_c(k, q) = \{H = (\mathcal{V}, \mathcal{E}) : H \text{ is } c\text{-uniform } \wedge |\mathcal{E}| - |\mathcal{V}| = q + 1 \wedge 1 \leq |\mathcal{E}| \leq k\},$$

where $c \geq 2, q \geq -c + 1, k \geq q + c + 1$ are fixed integers. $\mathcal{J}_c(k, q)$ contains $\mathcal{H}^c(k)$ as a subfamily. For this forbidden family, their upper bound is the following:

$$\text{ex}^*(m, \mathcal{J}_c(k, q)) = O(m^{c-1+\frac{1}{\lfloor \frac{k}{q+c+1} \rfloor}}). \tag{3.20}$$

For $q = 0$, (3.20) leads to

$$n(m, c, k) = O(m^{c-1+\frac{1}{\lfloor \frac{k}{c+1} \rfloor}}). \tag{3.21}$$

For $c \leq \left\lfloor \frac{k}{2} \right\rfloor - 1$, the upper bound in (3.21) significantly improves on the upper bound stated in Theorem 3.5.

Also, for $c = 2$, (3.21) yields a better upper bound ($O(m^{1+\frac{1}{\lfloor \frac{k}{3} \rfloor}})$) than the upper bound ($O(m^{1+\frac{1}{\lfloor \frac{k}{4} \rfloor}})$) we have obtained in Theorem 3.14. Here, we briefly show that the same upper bound, in terms of the order of magnitude, can be derived by direct application of an earlier result of [FS83]. Next, we state the required theorem of [FS83].

Let T be a tree [8] and v be a vertex outside of T. We construct a graph T' from T and v in the following manner. We consider T as a bipartite graph, and connect the vertices of one partition to v by vertex disjoint paths of length $\ell - 1$. Then we have the following upper bound.

Theorem 3.20 ([FS83])**.** $\text{ex}(m, T') = O(m^{1+\frac{1}{\ell}})$.

[8] A *tree* is a connected acyclic graph which can also be considered as a connected bipartite graph without cycles.

Remark 3.21. If we set $T = K_{1,2}$, and connect the two vertices of one partition with a vertex out of T, by two vertex disjoint paths of lengths $\ell - 1$, we get $T' = C_{2\ell}$. Then crux of Theorem 3.13, i.e., $\mathrm{ex}(m, C_{2\ell}) = O(m^{1+\frac{1}{\ell}})$ follows as corollary of Theorem 3.20.

Finally, we obtain the following improvement on the upper bound, obtained in Theorem 3.14.

Corollary 3.22. $n(m, 2, k) = O(m^{1+\frac{1}{\lfloor \frac{k}{3} \rfloor}})$.

Proof. We consider the graph $\theta(3, \lfloor \frac{k}{3} \rfloor)$. It has p edges and $p - 1$ vertices, where $p = 3\lfloor \frac{k}{3} \rfloor \leq k$. Now, we apply Theorem 3.20 with $T' = \theta(3, \lfloor \frac{k}{3} \rfloor)$, and the upper bound follows. □

For general c, our results show $n(m, c, k) = \Theta(m^c)$ for $k - \lceil \log k \rceil \leq c \leq k - 1$. For $c \leq k - \lceil \log k \rceil - 1$, exact order of magnitude of $n(m, c, k)$ is not known. However, for $c \leq \lfloor \frac{k}{2} \rfloor - 1$, orders of magnitude of upper and lower bounds on $n(m, c, k)$ are satisfactorily close; (3.11) shows $n(m, c, k) = \Omega(m^{c-1+\frac{c}{k-1}})$, whereas (3.21) shows $n(m, c, k) = O(m^{c-1+\frac{1}{\lfloor \frac{k}{c+1} \rfloor}})$. Now, the lower bound in (3.11), or even the weaker one in (3.10), are non-constructive. In fact, for $c \leq k - \lceil \log k \rceil - 1$ (except for $c = 2$), there is no non-trivial (in terms of order of magnitude of n) explicit construction of c-uniform CBCs in the literature. This motivates us to explicitly construct uniform CBCs with large value of n. We consider this problem in the next chapter.

Chapter 4

Derandomized Construction of Combinatorial Batch Codes

4.1 Introduction

In this chapter, we present explicit construction of uniform and almost regular CBCs. More precisely, we construct c-uniform (n, cn, k, m)-CBCs with $n = \Omega(m^{c-1+\frac{1}{k}})$ input data items. Constructed CBCs are almost regular. In particular, number of data items stored in each server is in the range $[\frac{nc}{m} - \sqrt{\frac{n}{2}\ln(4m)}, \frac{nc}{m} + \sqrt{\frac{n}{2}\ln(4m)}]$. Our construction is based on the randomized construction presented in [IKOS04a]. Our analysis of the construction of [IKOS04a] shows that the constructed CBCs are almost regular, an aspect that has so far not been addressed in the literature. On the other hand, derandomization of the randomized construction is indeed an explicit construction of c-uniform CBCs with $n = \Omega(m^{c-1+\frac{1}{k}})$. Before this, explicit construction of c-uniform CBCs, with similar order of magnitude of n, was not known for a wide range of values of c.

In this section, we cover the preliminaries, where we discuss the notion of explicit construction of a combinatorial object, setting and formulation of the construction problem, existing results related to the problem, and our contribution.

Section 4.2 comprises of the main technical part of this chapter, which includes proof of existence of a CBC with relevant parameters, derandomization of the proof, proof of correctness of the derandomization algorithm, and analysis of its runtime. Finally, in Section 4.3, we consider the possibility of a speed-up of the algorithm through parallelization.

4.1.1 Preliminaries

4.1.1.1 Notion of Explicit Construction

Construction of a combinatorial object with desirable properties is computation of a representation of the object by a deterministic algorithm and is tied with the resources used for the computation. In the literature, those constructions, which require practically feasible amount of resources, such as polynomial time or logarithmic space, are termed explicit. This can be contrasted with exhaustive search of a combinatorial object whose existence has been proven (e.g., by probabilistic argument); the search is done in the space of the object (i.e., the space from which the object is drawn) and requires infeasible amount of resources (e.g., exponential time). The notion of explicitness we will adhere to in this work is polynomial time constructibility, which requires that the time required for the construction by a deterministic algorithm be bounded by a polynomial in the size of the representation. Among numerous examples of explicit constructions, a notable one is Justesen's construction of asymptotically optimal explicit binary codes whose existence had been proven by Shannon by probabilistic argument. Explicitness is further classified as following.

– *Globally explicit.* In this case, the whole object is constructed in time polynomial in the size of the object. For example, a globally explicit construction of a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ would construct the adjacency matrix of the graph in time $poly(|\mathcal{V}|)$. However, the construction does not guarantee "quick" local access to individual members of the constructed object, which is necessary for practical applications. Hence, it is a weaker notion of construction (compared to the one discussed next) and often termed *weakly explicit*. Examples of constructions of this nature include *universal sets* and families of *perfect hash functions* in [NSS95], *subspace-evasive sets* in [PR04] and more recently in [BAS14], constructions for various restriction problems in [Bsh15], etc.

– *Locally explicit.* In this case, the idea is to have quick local access to the object. More formally, for a desirable combinatorial object $\mathcal{G}$, locally explicit construction of $\mathcal{G}$ is a deterministic algorithm that, given an index of size $\log(|\mathcal{G}|)$, outputs the member of $\mathcal{G}$ with the given index (or does some local computation on the member) in time $polylog(|\mathcal{G}|)$. This is more specialized notion and depends on the context. For example, a locally explicit construction of a d-regular graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ would list the neighbourhood of a vertex $v \in \mathcal{V}$ in time $poly(\log|\mathcal{V}|, \log d)$, given the index of v (which is of size $\log|\mathcal{V}|$). It is a stronger notion of construction (and hence termed *strongly explicit*) than the previous one, and is always desirable as it is useful for algorithmic applications. In fact, common notion of construction of combinatorial objects (e.g. using various algebraic structures) falls in this category.

4.1.1.2 SETTING AND THE PROBLEM

In this chapter, we will use the setting of Chapter 1. However, for the convenience of the reader, here, we provide a verbatim reproduction of the description of the setting from Chapter 1.

Let C be an (n, N, k, m)-CBC, with the set of input data items $\{x_1, \ldots, x_n\}$ and the set of servers $\{s_1, \ldots, s_m\}$. We represent C as a bipartite graph $\mathcal{G}_C = (\mathcal{L}, \mathcal{R}, \mathcal{E})$. Set of left vertices $\mathcal{L}$ represents $|\mathcal{L}| = n$ input data items, where vertex $u_i \in \mathcal{L}$ represents data item $x_i, 1 \leq i \leq n$. Set of right vertices $\mathcal{R}$ represents $|\mathcal{R}| = m$ servers, where vertex $v_j \in \mathcal{R}$ represents server $s_j, 1 \leq j \leq m$. $(u_i, v_j) \in \mathcal{E}$ is an edge in $\mathcal{G}_C$ if the data item x_i is stored in server s_j. Since the total storage is N, it follows that $\sum_{u \in \mathcal{L}} deg(u) = \sum_{v \in \mathcal{R}} deg(v) = |\mathcal{E}| = N$, where $deg(.)$ is the degree of a vertex in $\mathcal{G}_C$. Now, we observe that any subset $\{x_{i_1}, \ldots, x_{i_k}\}$ of k input data items can be retrieved by reading one item from each of k distinct servers $s_{i_1}, \ldots, s_{i_k}$ iff there are distinct $v_{i_1}, \ldots, v_{i_k} \in \mathcal{R}$ such that $v_{i_j} \in \Gamma(u_{i_j})$ for all $1 \leq j \leq k$, where $\Gamma(u_r)$, with $r \in \{1, \ldots, n\}$, is the *neighbourhood* of the vertex $u_r \in \mathcal{L}$. According to *Hall's theorem* (cf. [Bol86], pp. 6), this is equivalent to the condition that union of any j sets $\Gamma(u_{i_1}), \ldots \Gamma(u_{i_j})$ contains at least j elements for $1 \leq j \leq k$. These considerations lead naturally to the following theorem of [PSW09], which can also be thought as definition of a CBC.

Theorem 4.1 ([PSW09]). *A bipartite graph $\mathcal{G}_C = (\mathcal{L}, \mathcal{R}, \mathcal{E})$ represents an (n, N, k, m)-CBC C if and only if $|\mathcal{L}| = n$, $|\mathcal{R}| = m$, $|\mathcal{E}| = N$, and union of any collection of j sets $\Gamma(u_{i_1}), \ldots, \Gamma(u_{i_j})$, with $\{u_{i_1}, \ldots, u_{i_j}\} \subset \mathcal{L}$, contains at least j elements for $1 \leq j \leq k$.*

From now on, we will identify the graph $\mathcal{G}_C = (\mathcal{L}, \mathcal{R}, \mathcal{E})$ with an (n, N, k, m)-CBC, and omit the subscript C as it will not cause any confusion. We recall from Chapter 1 that a CBC $\mathcal{G} = (\mathcal{L}, \mathcal{R}, \mathcal{E})$ is called *c-uniform* if for each $u \in \mathcal{L}, deg(u) = c$, and it is called *$\ell$-regular* if for each $v \in \mathcal{R}, deg(v) = \ell$.

As discussed at the end of the previous chapter, the result that we obtain in this chapter, is motivated by the following problem: explicitly construct c-uniform (n, cn, k, k)-CBC with large value of n. Similar to the previous chapter, our setting of parameters is such that c and k are constants while m is variable. Also, similar to the previous chapter, we focus on the order of magnitude of n, expressed as a function of m, with c and k constants.

In the context of this problem, uniform CBCs resemble unbalanced expanders (resemblance of general batch codes with information dispersal problem was highlighted in Chapter 1), especially those constructed in [GUV09]. Next, we discuss this relationship.

Relation with unbalanced expanders. Expanders are sparse graphs with high connectivity. These graphs have found numerous applications in different areas, especially in theoretical computer science (see [HLW06]). Existence of expanders, with favourable parameters, is easy to prove through probabilistic arguments; however, their explicit construction is a very difficult task.

There are different notions of expansion of an expander. In one of the formulations, the term refers to graphs with linear (in terms of the number of vertices) number of edges, where each small subset of vertices 'expands', i.e., has many neighbours. For a bipartite graph $\mathcal{G} = (\mathcal{L}, \mathcal{R}, \mathcal{E})$, the condition is that each small subset of vertices of one of the partite sets (typically the left partite set $\mathcal{L}$) has many neighbours in the other partite set (typically the right partite set $\mathcal{R}$). More specifically, an $(n, m, c, \gamma, \alpha)$-expander is a bipartite graph $G = (\mathcal{L}, \mathcal{R}, \mathcal{E})$ with the following properties: (i) $|\mathcal{L}| = n$, (ii) $|\mathcal{R}| = m$, (iii) for each vertex $v \in \mathcal{L}, deg(v) = c$, (iv) for each $\mathcal{S} \subseteq \mathcal{L}$, with $|\mathcal{S}| \leq \gamma n, |\Gamma(\mathcal{S})| \geq \alpha n$. Expanders with $n > m$ are termed 'unbalanced'. They have many applications, especially in the construction of asymptotically good error-correcting codes ([SS96]), space efficient storage schemes ([BMRV02]), etc.

c-uniform CBCs can be naturally viewed as unbalanced expander with expansion $\alpha = 1$. Both are bipartite graphs with constant left-degree c. In both the cases, it is required that every subset of vertices $\mathcal{L}$, of up to a specified size, should have neighbourhood in $\mathcal{R}$ with certain minimum cardinality. Also, in both the cases, it is desirable that $|\mathcal{L}| >> |\mathcal{R}|$.

However, the dissimilarities are more significant. In the case of unbalanced expanders, the goal is to stretch the expansion α, of subsets (of specified sizes) of $\mathcal{L}$, as close to the left-degree c as possible (typically, $\alpha = c(1-\varepsilon)$ for any $\varepsilon > 0$). Whereas, in case of CBCs, expansion $\alpha = 1$ is sufficient. On the other hand, for CBCs, it is more important to make $|\mathcal{L}|$ as large as possible with respect to $|\mathcal{R}|$. Also, the parameter k is a constant in case of CBCs (within our setting of parameters). Whereas, for unbalanced expanders, k varies with n. These differences make the (desirable) parameters in these two cases essentially unrelated. For example, it will be shown later that by relaxing α to 1, it is possible to achieve much higher values of n than obtained in the construction of [GUV09]. Dependence of k on n, in [GUV09], makes it essential (by a result of [RTS00]) for the left-degree c to be $poly(\log n)$. Whereas, in case of CBCs (within our setting), c is a constant independent of n.

Therefore, it is unlikely that the construction of unbalanced expander from [GUV09] (or any other method of construction of unbalanced expanders) can be immediately used for construction of c-uniform (n, cn, k, m)-CBCs, where c and k are constants independent of m.

4.1.2 EXISTING RESULTS

To set the context for our results, we briefly recall existing results, pertaining to bounds on $n(m, c, k)$.

(*i*) In [IKOS04a], the authors have shown, using probabilistic method, that $n(m, c, k) = \Omega(m^{c-1})$. In [PSW09], the authors have refined the above estimate, using the *method of deletion* (another probabilistic technique, see [AS00]), to $n(m, c, k) = \Omega(m^{\frac{ck}{k-1}-1})$. They have also shown, through explicit construction, that $n(m, k-1, k) = (k-1)\binom{m}{k-1}$ and $n(m, k-2, k) = \binom{m}{k-2}$.

(*ii*) In the previous chapter, we have shown that $n(m,c,k) = O(m^{c-\frac{1}{2^{c-1}}})$ for $7 \leq k$, and $3 \leq c \leq k - \lceil \log k \rceil - 1$. Also, for $k - \lceil \log k \rceil \leq c \leq k-1$, we have shown, through explicit construction, that $n(m,c,k) = \Theta(m^c)$. For $c = 2$ case, we have improved the lower bound (stated above) of [PSW09], through explicit construction, to $n(m,2,k) = \Omega(m^{\frac{k+1}{k-1}})$ for all $k \geq 8$ and infinitely many values of m.

(*iii*) In [BT15], the authors have improved the general upper bound to show that $n(m,c,k) = O(m^{c-1+\frac{1}{\lfloor \frac{k}{c+1} \rfloor}})$ for $c \leq \frac{k}{2} - 1$.

All the explicit constructions, mentioned above, are locally explicit. The above results show $n(m,c,k) = \Theta(m^c)$ for $k - \lceil \log k \rceil \leq c \leq k-1$. For $c \leq k - \lceil \log k \rceil - 1$, exact order of magnitude of $n(m,c,k)$ is not known. However, for $c \leq \lfloor \frac{k}{2} \rfloor - 1$, orders of magnitude of upper and lower bounds on $n(m,c,k)$ are satisfactorily close; namely $n(m,c,k) = \Omega(m^{c-1+\frac{c}{k-1}})$ and $n(m,c,k) = O(m^{c-1+\frac{1}{\lfloor \frac{k}{c+1} \rfloor}})$ respectively. Now, the lower bound $n(m,c,k) = \Omega(m^{c-1+\frac{c}{k-1}})$, or even the weaker one $n(m,c,k) = \Omega(m^{c-1})$, are non-constructive. In fact, for $c \leq k - \lceil \log k \rceil - 1$ (except for $c = 2$), there is no non-trivial (in terms of order of magnitude of n) explicit construction of c-uniform CBCs in the literature.[1]

All of the above results pertain to uniform CBCs only. CBCs, which are both uniform and regular, have not been considered in the literature so far. Study of uniform and regular CBCs is theoretically interesting for its own sake. Moreover, in case of regular CBCs, number of data items stored in each server is the same. Hence, it is easier to allocate storage uniformly and optimally across different servers. This is very useful, especially under dynamic conditions, where the database (i.e., the set of distinct data items to be stored) changes with addition and deletion of data items.

Above considerations motivate us to explicitly construct uniform CBCs with large value of n, which are both uniform and regular.

[1] In [SG14], constructions of CBCs are given for a setting of parameters where k and c vary with m. Since in our setting we require k and c to be constants, we do not discuss the results of [SG14].

4.1.3 OUR CONTRIBUTION

We construct c-uniform (n, cn, k, m)-CBCs, where $n = \Omega(m^{c-1+\frac{1}{k}})$. These CBCs are almost regular; for these CBCs, number of data items stored in each server is $\frac{nc}{m} + o(n)$. Here, we point out that for regular CBCs, with same parameters, this value is exactly $\frac{nc}{m}$. Formal statement of our result is the following.

Theorem 4.2. *Let c, k be positive constants. Then for all sufficiently large m, there exists c-uniform (n, cn, k, m)-CBC, where $n = \Omega(m^{c-1+\frac{1}{k}})$, and number of items in each server is in the range $\left[\frac{nc}{m} - \sqrt{\frac{n}{2}\ln(4m)}, \frac{nc}{m} + \sqrt{\frac{n}{2}\ln(4m)}\right]$. Moreover, there is a globally explicit construction of the CBC that runs in $poly(m)$ time.*

We use the randomized construction of uniform CBCs, given in [IKOS04a], and analyze it in greater detail. Our analysis shows almost regularity of the constructed CBCs. Also, we observe that, for the constructed CBCs, $n = \Omega(m^{c-1+\frac{1}{k}})$, as opposed to $n = \Omega(m^{c-1})$, shown in [IKOS04a]. Then we derandomize the construction using the *method of conditional expectation* (see [AS00]). Our analysis of the runtime of the derandomization shows that the derandomization is indeed a globally explicit construction of CBCs. Order of magnitude of n $(= \Omega(m^{c-1+\frac{1}{k}}))$, of our constructed CBCs, is inferior to that $(= \Omega(m^{c-1+\frac{c}{k-1}}))$ of [PSW09]. However, we point out that our construction is explicit, and the constructed CBCs are uniform and almost regular. It is not known whether these properties are there in the construction of [PSW09].

To describe our construction, we provide a deterministic algorithm with the following properties.

(i) The algorithm is given as input integers k, c, and sufficiently large m;

(ii) it runs in time $poly(m)$;

(iii) it outputs the edges of a bipartite graph $(\mathcal{L}, \mathcal{R}, \mathcal{E})$, with $|\mathcal{R}| = m$, $|\mathcal{L}| = n = \frac{m^{c-1+\frac{1}{k}}}{4k^{c+1}}$; the bipartite graph satisfies the following conditions,

- (a) each vertex in $\mathcal{L}$, has degree c, and each vertex in $\mathcal{R}$,has degree in the range $\left[\frac{nc}{m} - \sqrt{\frac{n}{2}\ln(4m)}, \frac{nc}{m} + \sqrt{\frac{n}{2}\ln(4m)}\right]$,
- (b) each subset of $i, 1 \leq i \leq k$, vertices in $\mathcal{L}$, has at least i neighbours in $\mathcal{R}$.

Here, we point out that there is a trivial non-explicit algorithm to construct the required bipartite graph. For the given input parameters, the algorithm searches the space of all possible bipartite graphs $(\mathcal{L}, \mathcal{R}, \mathcal{E})$, with $|\mathcal{R}| = m$, $|\mathcal{L}| = n = \frac{m^{c-1+\frac{1}{k}}}{4k^{c+1}}$, and outputs one that satisfies the conditions (a) and (b). The algorithm runs in time exponential in m. Hence, it is non-explicit.

In the proof of Theorem 4.2, we use various probabilistic methods. These methods are standard in the literature. We refer the reader to [AS00] for relevant background. In particular, we need the following version of Hoeffding's inequality.

Theorem 4.3 (Hoeffding's inequality[Hoe63]). *Let $X_1, X_2, \ldots, X_n$ be independent random variables taking their values in the interval $[0, 1]$. Let $X = \sum_i X_i$. Then for every real number $a > 0$,* $\mathbf{Pr}\{|X - \mathbf{E}[X]| \geq a\} \leq 2e^{\frac{-2a^2}{n}}$.

Also, given a set $\mathcal{S}$ and a positive integer $c(\leq |\mathcal{S}|)$, we will denote by $\binom{\mathcal{S}}{c}$, the set of all c element subsets of $\mathcal{S}$.

4.2 PROOF OF THEOREM 4.2

We split the proof of Theorem 4.2 into two parts. In the first part, we give probabilistic proof of existence of the CBC. This proof is essentially a randomized construction of the CBC. In the second part, we derandomize the construction using the method of conditional expectation. This is a standard method to derandomize a randomized algorithm. It has its genesis in [ES73]. It was later on applied to prove many other derandomization results (e.g. [Rag88, Spe94]). Informally, the method systematically performs a binary (or more commonly a d-ary) search on the sample space, from where the corresponding randomized algorithm makes its choices, for a "good point". Due to this systematic search, it finds a good point "quickly".

Proof of existence. We construct a bipartite graph $\mathcal{G} = (\mathcal{L}, \mathcal{R}, \mathcal{E})$, where $\mathcal{L}$ is the set $\{u_1, \ldots, u_n\}$ of n left vertices, $\mathcal{R}$ is the set $\{v_1, \ldots, v_m\}$ of m right vertices, and $\mathcal{E}$ is the set of edges, in the following manner. For each vertex in $\mathcal{L}$, we choose its c distinct neighbours by picking randomly, uniformly, and independently a subset of c vertices from $\mathcal{R}$. So, neighbourhood of the vertex is an independently and uniformly chosen random element of $\binom{\mathcal{R}}{c}$.

Hence, for $u \in \mathcal{L}, S' \subseteq \mathcal{R}$,

$$\mathbf{Pr}\{\Gamma(u) \subseteq S'\} = \frac{\binom{|S'|}{c}}{\binom{m}{c}} \leq \left(\frac{|S'|}{m}\right)^c .$$

Next, for a subset $S \subset \mathcal{L}$, with $|S| = i, c+1 \leq i \leq k$, and a subset $S' \subset \mathcal{R}$, with $|S'| = i-1$, we say that event $Bad_{S,S'}$ has occured if $\Gamma(S) \subseteq S'$. So, we have

$$\mathbf{Pr}\{Bad_{S,S'}\} \leq \left(\frac{i-1}{m}\right)^{ic} , \tag{4.1}$$

using independence of the events $\Gamma(u) \subseteq S'$ for $u \in \mathcal{L}$. Now, our goal is to bound the probability of occurrence of any $Bad_{S,S'}$, with $S \subset \mathcal{L}$, $S' \subset \mathcal{R}$, and $c+1 \leq i \leq k$. To this end, we have

$$\begin{aligned}
\sum_{c+1\leq i\leq k} \sum_{\substack{S\subset\mathcal{L},\\ |S|=i}} \sum_{\substack{S'\subset\mathcal{R},\\ |S'|=i-1}} \mathbf{Pr}\{Bad_{S,S'}\} &\leq \sum_{c+1\leq i\leq k} \binom{n}{i}\binom{m}{i-1}\left(\frac{i-1}{m}\right)^{ic} \\
&\leq \sum_{1\leq i\leq k} n^i m^{i-1}\left(\frac{i-1}{m}\right)^{ic} \\
&\leq \sum_{1\leq i\leq k} n^i m^{i-1}\left(\frac{k}{m}\right)^{ic} \\
&\leq \sum_{1\leq i\leq k} \left(\frac{1}{4k}\right)^i \quad \text{since } n = \frac{m^{c-1+\frac{1}{k}}}{4k^{c+1}} \\
&\leq \frac{1}{4} .
\end{aligned} \tag{4.2}$$

Next, for $u \in \mathcal{L}, v \in \mathcal{R}$, we define the indicator random variable X_v^u such that

$$X_v^u = \begin{cases} 1 & (u,v) \in \mathcal{E} \\ 0 & \text{otherwise.} \end{cases}$$

Also, let $X_v, v \in \mathcal{R}$, be a random variable denoting the degree of vertex v. Clearly, $X_v = \sum_{u\in\mathcal{L}} X_v^u$. Now, $\mathbf{Pr}\{X_v^u = 1\} = \frac{c}{m}$. So, by linearity of expectation, we have

$$\mathbf{E}[X_v] = \mathbf{E}\left[\sum_{u\in\mathcal{L}} X_v^u\right] = \sum_{u\in\mathcal{L}} \mathbf{E}[X_v^u] = \frac{nc}{m} .$$

Since the neighbourhoods of vertices $u \in \mathcal{L}$ are chosen independently, it follows that the variables X_v^u, with $u \in \mathcal{L}$, and a fixed $v \in \mathcal{R}$, are mutually independent.

So, by applying Theorem 4.3, with $a = \sqrt{\frac{n}{2}\ln(4m)}$, we have

$$\mathbf{Pr}\left\{|X_v - \mathbf{E}[X_v]| \geq \sqrt{\frac{n}{2}\ln(4m)}\right\} \leq 2(4m)^{-1} \leq \frac{1}{2m}\,. \tag{4.3}$$

By union bound, the probability, that the event $|X_v - \mathbf{E}[X_v]| \geq \sqrt{\frac{n}{2}\ln(4m)}$ occurs for some $v, v \in \mathcal{R}$, is bounded by

$$\sum_{v\in\mathcal{R}} \mathbf{Pr}\left\{|X_v - \mathbf{E}[X_v]| \geq \sqrt{\frac{n}{2}\ln(4m)}\right\} \leq \frac{1}{2}\,. \tag{4.4}$$

Hence, from equations (4.2) and (4.4), with probability at least $1 - (\frac{1}{4} + \frac{1}{2}) = \frac{1}{4}$, none of the above events occur. □

Derandomization. The derandomization algorithm has n iterations. At the beginning of t-th iteration, with $1 \leq t \leq n$, neighbourhoods of vertices $u_1, \ldots, u_{t-1} \in \mathcal{L}$ are fixed. At the t-th iteration, $\Gamma(u_t) \in \binom{\mathcal{R}}{c}$ (i.e., neighbourhood of u_t) is fixed in such a way that minimizes the expected number of violations of conditions (a) and (b) stated before (in Section 4.1.3). Before we present the derandomization algorithm, we derive expressions for (i) the expected number of $Bad_{S,S'}$ events, and (ii) the expected number of vertices $v \in \mathcal{R}$, for which $|deg(v) - \frac{nc}{m}| > \sqrt{\frac{n}{2}\ln(4m)}$, conditional on fixed choices of $\Gamma(u_1), \ldots, \Gamma(u_t)$.Then we show that if at t-th iteration, with $1 \leq t \leq n$, with $\Gamma(u_1), \ldots, \Gamma(u_{t-1})$ already fixed, the algorithm selects $\Gamma(u_t)$ in such a way to minimize the sum of these two expectations, then in the final graph (which is no longer random since all the neighbourhoods are fixed), there are (i) no $Bad_{S,S'}$ events, and (ii) no vertices $v \in \mathcal{R}$ for which $|deg(v) - \frac{nc}{m}| > \sqrt{\frac{n}{2}\ln(4m)}$. So, there are no violations of conditions (a) and (b). Now, the algorithm (Algorithm 1) follows immediately from these observations.

Let us define indicator random variables $Y_{S,S'}$ corresponding to each event $Bad_{S,S'}$, i.e.,

$$Y_{S,S'} = \begin{cases} 1 & \text{if } \Gamma(S) \subseteq S' \\ 0 & \text{otherwise.} \end{cases}$$

Also, we define $Y = \sum_{c+1\le i\le k} \sum_{\substack{S\subset\mathcal{L},\\|S|=i}} \sum_{\substack{S'\subset\mathcal{R},\\|S'|=i-1}} Y_{S,S'}$. By linearity of expectation, we have

$$\begin{aligned}\mathbf{E}[Y] &= \mathbf{E}\left[\sum_{c+1\le i\le k} \sum_{\substack{S\subset\mathcal{L},\\|S|=i}} \sum_{\substack{S'\subset\mathcal{R},\\|S'|=i-1}} Y_{S,S'}\right] \\ &= \sum_{c+1\le i\le k} \sum_{\substack{S\subset\mathcal{L},\\|S|=i}} \sum_{\substack{S'\subset\mathcal{R},\\|S'|=i-1}} \mathbf{E}[Y_{S,S'}] \\ &= \sum_{c+1\le i\le k} \sum_{\substack{S\subset\mathcal{L},\\|S|=i}} \sum_{\substack{S'\subset\mathcal{R},\\|S'|=i-1}} \mathbf{Pr}\{Y_{S,S'}\} \le \frac{1}{4} \text{ from (4.2).}\end{aligned}$$

Let $C_1, C_2, \ldots, C_t \in \binom{\mathcal{R}}{c}$ be fixed subsets such that $\Gamma(u_j) = C_j$, with $1 \le j \le t$. Neighbourhoods of the remaining vertices in $\mathcal{L}$ are chosen independently and uniformly at random from $\binom{\mathcal{R}}{c}$. Let $S \subseteq \mathcal{L}, S' \subseteq \mathcal{R}$, with $|S| = i$, and $|S'| = i-1$, be fixed subsets, where $c+1 \le i \le k$. Also, let $W = S \cap \{u_1, u_2, \ldots, u_t\}$, where $|W| = w$ and $\Gamma(W) = \emptyset$ for $W = \emptyset$. Then, we have

$$\begin{aligned}&\mathbf{E}[Y_{S,S'}|\Gamma(u_1) = C_1, \ldots, \Gamma(u_t) = C_t] \\ &= \mathbf{Pr}\{\Gamma(S) \subseteq S'|\Gamma(u_1) = C_1, \ldots, \ldots \Gamma(u_t) = C_t\} \\ &= \begin{cases} 0 & \text{if } \Gamma(W) \not\subseteq S' \\ \left(\frac{\binom{i-1}{c}}{\binom{m}{c}}\right)^{i-w} & \text{otherwise.}\end{cases}\end{aligned} \tag{4.5}$$

So, by applying linearity of expectation, and from (4.5), we have

$$\begin{aligned}&\mathbf{E}[Y|\Gamma(u_1) = C_1, \ldots, \Gamma(u_t) = C_t] \\ &= \sum_{c+1\le i\le k} \sum_{\substack{S\subset\mathcal{L},\\|S|=i}} \sum_{\substack{S'\subset\mathcal{R},\\|S'|=i-1}} \mathbf{E}[Y_{S,S'}|\Gamma(u_1) = C_1, \ldots, \ldots \Gamma(u_t) = C_t] \\ &= \sum_{c+1\le i\le k} \sum_{\substack{S\subset\mathcal{L},\\|S|=i}} \sum_{\substack{S'\subset\mathcal{R},\\|S'|=i-1}} \mathbf{Pr}\{\Gamma(S) \subseteq S'|\Gamma(u_1) = C_1, \ldots, \ldots \Gamma(u_t) = C_t\} \\ &= \sum_{c+1\le i\le k} \sum_{\substack{S\subset\mathcal{L},\\|S|=i}} \sum_{\substack{S'\subset\mathcal{R},\\|S'|=i-1\\\Gamma(W)\subseteq S'}} \left(\frac{\binom{i-1}{c}}{\binom{m}{c}}\right)^{i-w}.\end{aligned} \tag{4.6}$$

Next, corresponding to each vertex $v \in \mathcal{R}$, we introduce an indicator random variable Z_v, such that

$$Z_v = \begin{cases} 1 & |deg(v) - \frac{nc}{m}| > \sqrt{\frac{n}{2}\ln(4m)} \\ 0 & \text{otherwise.} \end{cases}$$

Let $Z = \sum_{v \in \mathcal{R}} Z_v$. So, by linearity of expectation, we have

$$\mathbf{E}[Z] = \mathbf{E}\left[\sum_{v\in\mathcal{R}} Z_v\right] = \sum_{v\in\mathcal{R}} \mathbf{E}[Z_v] = \sum_{v\in\mathcal{R}} \mathbf{Pr}\{Z_v = 1\} \leq \frac{1}{2}\ , \text{ from (4.4).}$$

Like in the previous case, we estimate $\mathbf{E}[Z|\Gamma(u_1) = C_1, \ldots, \Gamma(u_t) = C_t]$, by estimating $\mathbf{E}[Z_v|\Gamma(u_1) = C_1, \ldots, \Gamma(u_t) = C_t]$ for each $v \in \mathcal{R}$. For a fixed $v \in \mathcal{R}$, let $\ell = |\{u_i | v \in \Gamma(u_i), 1 \leq i \leq t\}|$. Also, let $\alpha = \frac{nc}{m} - \sqrt{\frac{n}{2}\ln(4m)}$, and $\beta = \frac{nc}{m} + \sqrt{\frac{n}{2}\ln(4m)}$. Then, we have

$$\begin{aligned}
&\mathbf{E}[Z|\Gamma(u_1) = C_1, \ldots, \Gamma(u_t) = C_t] \\
&= \sum_{v\in\mathcal{R}} \mathbf{E}[Z_v|\Gamma(u_1) = C_1, \ldots, \Gamma(u_t) = C_t] \\
&= \sum_{v\in\mathcal{R}} \mathbf{Pr}\{deg(v) < \alpha - \ell \text{ or } deg(v) > \beta - \ell | \Gamma(u_1) = C_1, \ldots, \Gamma(u_t) = C_t\} \\
&= \sum_{v\in\mathcal{R}} \Bigg(\sum_{i=0}^{i=\alpha-\ell-1} \binom{n-t}{i} \left(\frac{c}{m}\right)^i \left(1 - \frac{c}{m}\right)^{n-t-i} + \\
&\sum_{i=\beta-\ell+1}^{n-t} \binom{n-t}{i} \left(\frac{c}{m}\right)^i \left(1 - \frac{c}{m}\right)^{n-t-i} \Bigg) . \qquad (4.7)
\end{aligned}$$

Finally, we show that if at t-th iteration, with fixed $\Gamma(u_1) = C_1, \ldots, \Gamma(u_{t-1}) = C_{t-1}$ at the beginning, $\Gamma(u_t) = C_t$ is chosen so as to minimize $\mathbf{E}[Y + Z|\Gamma(u_1) = C_1, \ldots, \Gamma(u_t) = C], C \in \binom{\mathcal{R}}{c}$, then in the final graph (which is no longer random) conditions (a) and (b) are satisfied. To this end, we first observe that

$$\begin{aligned}
&\mathbf{E}[Y + Z|\Gamma(u_1) = C_1, \ldots, \Gamma(u_{t-1}) = C_{t-1}] \\
=&\frac{1}{\binom{m}{c}} \sum_{C\in\binom{\mathcal{R}}{c}} \mathbf{E}[Y + Z|\Gamma(u_1) = C_1, \ldots, \Gamma(u_t) = C] \\
&\geq \min_{C\in\binom{\mathcal{R}}{c}} \mathbf{E}[Y + Z|\Gamma(u_1) = C_1, \ldots, \Gamma(u_t) = C] . \qquad (4.8)
\end{aligned}$$

Hence, it follows that

$$\begin{aligned}
&\min_{C_1,\ldots,C_n\in\binom{\mathcal{R}}{c}} \mathbf{E}[Y+Z|\Gamma(u_1)=C_1,\ldots,\Gamma(u_n)=C_n] \\
&\leq \min_{C_1,\ldots,C_{n-1}\in\binom{\mathcal{R}}{c}} \mathbf{E}[Y+Z|\Gamma(u_1)=C_1,\ldots,\Gamma(u_{n-1})=C_{n-1}] \\
&\vdots \\
&\leq \min_{C_1\in\binom{\mathcal{R}}{c}} \mathbf{E}[Y+Z|\Gamma(u_1)=C_1] \leq \mathbf{E}[Y+Z] \leq \frac{3}{4}\,. \qquad (4.9)
\end{aligned}$$

Since Y and Z are integer valued random variables, (4.9) implies that, at the end, with $\Gamma(u_1),\ldots,\Gamma(u_n)$ fixed, $Y=0$ and $Z=0$. So, the conditions (a) and (b) are met. Now, we have the following algorithm to construct the bipartite graph.

Algorithm 1: Algorithm to construct uniform and almost regular CBC

Input: Positive constants c, k, and sufficiently large m.
Output: A bipartite graph $(\mathcal{L},\mathcal{R},\mathcal{E})$, where
$\mathcal{L}=\{u_1,u_2,\ldots,u_n\}(n=\frac{m^{c-1+\frac{1}{k}}}{4k^{c+1}})$ and $\mathcal{R}=\{v_1,v_2,\ldots,v_m\}$ such that $\Gamma(u_j)=C_j\in\binom{\mathcal{R}}{c}, 1\leq j\leq n$ meeting conditions (a) and (b).

$\alpha=\frac{nc}{m}-\sqrt{\frac{n}{2}\ln(4m)}$, and $\beta=\frac{nc}{m}+\sqrt{\frac{n}{2}\ln(4m)}$;
for $j\leftarrow 1$ **to** n **do**
  $U_{j-1}=\{u_1,u_2,\ldots,u_{j-1}\}, min\leftarrow 1$
  for $C\in\binom{\mathcal{R}}{c}$ **do**

$$Y'\leftarrow \sum_{c+1\leq i\leq k}\ \sum_{\substack{u_j\in S\subset\mathcal{L},\\ |S|=i}}\ \sum_{\substack{S'\subset\mathcal{R},\\ |S'|=i-1\\ \Gamma(U_{j-1}\cap S)\cup C\subseteq S'}} \left(\frac{\binom{i-1}{c}}{\binom{m}{c}}\right)^{i-|U_{j-1}\cap S|-1}$$

$$Z\leftarrow \sum_{v\in\mathcal{R}}\Bigg(\sum_{i=0}^{\alpha-|U_{j-1}\cap\Gamma(v)|-|\{v\}\cap C|-1}\binom{n-j}{i}\left(\frac{c}{m}\right)^i\left(1-\frac{c}{m}\right)^{n-j-i} + \sum_{i=\beta-|U_{j-1}\cap\Gamma(v)|-|\{v\}\cap C|+1}^{n-j}\binom{n-j}{i}\left(\frac{c}{m}\right)^i\left(1-\frac{c}{m}\right)^{n-j-i}\Bigg)$$

    if $min>Y'+Z$ **then**
      $\Gamma(u_j)=C$
      $min\leftarrow Y'+Z$
    end
  end
end

Proof of correctness of the algorithm. At the beginning of the j-th iteration, $\Gamma(u_1) = C_1, \ldots, \Gamma(u_{j-1}) = C_{j-1}$ are fixed, and the algorithm selects $C = C_j$, which minimizes $Y' + Z$ for given $\Gamma(u_1) = C_1, \ldots, \Gamma(u_j) = C$. We note that according to (4.5), $\mathbf{E}[Y_{S,S'}|\Gamma(u_1) = C_1, \ldots, \Gamma(u_j) = C_j]$ is independent of the particular choice of C_j if $u_j \notin S$. So, in the j-th iteration of the algorithm, while computing Y', only those summands $\mathbf{E}[Y_{S,S'}|\Gamma(u_1) = C_1, \ldots, \Gamma(u_j) = C]$ are considered for which $u_j \in S$. Hence, $Y' \leq \mathbf{E}[Y_{S,S'}|\Gamma(u_1) = C_1, \ldots, \Gamma(u_j) = C]$, and the particular choice of $C = C_j$, which minimizes $Y' + Z$ for given $\Gamma(u_1) = C_1, \ldots, \Gamma(u_{j-1}) = C_{j-1}, \Gamma(u_j) = C$, also minimizes $\mathbf{E}[Y + Z|\Gamma(u_1) = C_1, \ldots, \Gamma(u_{j-1}) = C_{j-1}, \Gamma(u_j) = C]$. This, along with (4.9), also justifies setting min to 1 at the beginning of j-th iteration. Hence, the proof follows from the discussion preceding Algorithm 1.

Runtime of the algorithm. Now, we present a coarse analysis of the runtime of the algorithm, which is sufficient to indicate that the algorithm runs in time $poly(m)$. For our analysis, we consider the RAM model of computation. In this model, addition, multiplication, and division are atomic operations, i.e., these operations are assumed to take unit time. We refer the reader to [MR95] for further details about this model.

First, we estimate the time required by the algorithm to compute Y'. We observe that, by using dynamic programming, the time required to compute $\binom{m}{c}$ and $\binom{i-1}{c}$ is $O(m^2)$. The exponentiation takes time $O(\log k)$. These operations are repeated $O(kn^{k-1}m^{k-1})$ times to get the summation. So, the time required by the algorithm to compute Y' is $O(m^{(c+1)(k-1)+2})$. Similarly, in the case of computing Z, computation of binomial coefficients $\binom{n-i}{j}$ takes time $O(n^2)$. The exponentiations take time $O(\log n)$. Hence, the time required to compute Z is $O(mn^3 \log n) = O(m^{3c-1} \log m)$. These two steps, i.e., computation of Y' and Z, are repeated $O(nm^c) = O(m^{2c})$ times. So, overall time complexity of the algorithm is $O(m^{(k+1)(c+1)})$.

Therefore, Algorithm 1 is indeed a globally explicit construction of c-uniform (n, cn, k, m)-CBCs, with $n = \Omega(m^{c-1+\frac{1}{k}})$ and number of data items stored in each server in the range $[\frac{nc}{m} - \sqrt{\frac{n}{2}\ln(4m)}, \frac{nc}{m} + \sqrt{\frac{n}{2}\ln(4m)}]$.

4.3 CONCLUDING REMARKS

Limitations of the construction. Here, we point out the following limitations of our construction.

(*a*) Our runtime analysis of Algorithm 1 shows that efficiency of the algorithm crucially depends on k. Runtime of the algorithm is $poly(m)$ if and only if k is constant. This limits applicability of Algorithm 1 to wider setting where k is allowed to vary.

(*b*) The construction is globally explicit. As discussed in the beginning, this is a weaker notion of explicitness.

(*c*) Analysis of the runtime of Algorithm 1 shows that its time complexity ($O(m^{(k+1)(c+1)})$) is relatively higher, even in terms of the number of edges (which is $O(m^c)$). One of the reasons for this is the sequential nature of the algorithm. A possible approach to speed-up the construction is to derandomize the parallel randomized construction presented in the first part of Theorem 4.2, i.e., in the proof of existence of the CBC. Next, we briefly explore this possibility.

Towards derandomization in NC. First, we observe that the construction can be carried out on a probabilistic Parallel Random Access Machine (PRAM) (cf. [MR95]). The probabilistic PRAM constructs the CBC in constant time using $n = poly(m)$ many processors. Indeed, for each of the n items we allocate one processor. These n processors make their random choices parallelly in constant time. So, the construction is in *RNC*.[2] It is naturally interesting to investigate *NC*-derandomization of problems in *RNC*. In such derandomization, the same problem is solved using a deterministic PRAM subject to same set of restrictions on resources. Two of the most commonly used techniques employed for such derandomization are the method of conditional expectation and the *method of small sample spaces* (see [AS00]). Sometimes they are used together [BR91, MNN94]. Next, we very briefly and informally describe these two methods

We first point out that, in order to (completely) derandomize a randomized algorithm, it is sufficient to deterministically and quickly find a good point in the sample space, from which the randomized algorithm makes its random choices.

[2] In fact, the construction is in *ZNC* with the expected number of iterations at most 4.

As we have discussed and shown (in Algorithm 1) earlier, in the method of conditional expectation, a binary search (or more commonly a d-ary search) is performed in the sample space for a good point. Due to binary search a good point is found out quickly. On the other hand, method of small sample spaces is applicable when the randomized algorithm involves random variables that require limited independence among themselves. It is known that random variables, with limited (typically, constant) independence, can be defined over a (appropriately chosen) small sized (polynomial in the number of variables) sample space. So, the randomized algorithm can be executed using such a small sized sample space. Now, it is possible to deterministically find a good point from the sample space by exhaustive search. Since the sample space is small, i.e., polynomial sized, the exhaustive search can be done quickly, i.e., in polynomial time. Thus, we finally have a deterministic algorithm, which runs in polynomial time.

In the proof of Theorem 4.2, we have used independence twice: (*i*) in (4.1), we have used k-wise independence, and (*ii*) in (4.3), we used n-wise independence among random variables $X_1, \ldots, X_n$ for application of Hoeffding's inequality (Theorem 4.3).[3] However, such independence comes at the cost of a large sample space. More precisely, in [ABI86], it was shown that, in order to ensure k-wise independence among n random variables, the sample space size has to be $\Omega(n^{\frac{k}{2}})$. So, in case of Theorem 4.2, requirement on the size of sample space is huge ($\Omega(m^m)$). However, we observe that the requirement of n-wise independence in Theorem 4.2 can be brought down to $O(\ln(m))$-wise independence with the help of following limited independence Chernoff bound. First, we state the bound.

Theorem 4.4 ([BR94]). *Let $t \geq 4$ be an even integer. Suppose $X_1, \ldots, X_n$ are t-wise independent random variables taking values in $[0, 1]$. Let $X = X_1 + \cdots + X_n$, and $a > 0$. Then*

$$\mathbf{Pr}\{|X - \mathbf{E}[X]| \geq a\} \leq C_t \left(\frac{nt}{a^2}\right)^{\frac{t}{2}},$$

where C_t is a constant depending on t, and $C_t < 1$ for $t \geq 6$.

Now, in (4.3), we need $\frac{1}{2m}$ in the r.h.s. This is possible by setting $t = 2\ln(2m)$ (for simplicity we assume $2\ln(2m)$ is even) and $a = \sqrt{2en\ln(2m)}$ in Theorem 4.4.

[3] Here, we again point out that k-wise independence in choices of $\Gamma(u), u \in \mathcal{L}$ induces k-wise independence among random variables $X_v^u, u \in \mathcal{L}$ for fixed $v \in \mathcal{R}$. Though the events and random variables are different in two cases.

Hence, $O(\ln(m))$-wise independence, in choosing $\Gamma(u)$ for $u \in \mathcal{L}$, is sufficient for the randomized construction (with somewhat inferior bound on the deviation of the degrees from the average).

In [BR91, MNN94], the authors developed frameworks for *NC*-derandomization of certain algorithms (notably, the set discrepancy problem of Spencer [Spe94]). These algorithms require $O(\log^c(n))$-wise independence among n random variables, where c is a constant. One of the vital points of these frameworks is parallel computation of relevant conditional expectations of limited independence random variables in logarithmic time. In case of Algorithm 1, this means computation of Y' and Z by $poly(m)$ processors, in $polylog(m)$ time, under $O(\ln(m))$-wise independence among random choices of $\Gamma(u)$ for $u \in \mathcal{L}$. At present, it is not clear to us how this can be achieved in the frameworks of [BR91, MNN94], and seems to require a more specialized technique.

Appendix A

Graphs and Hypergraphs: Definitions and Notations

Here, we recall some standard definitions of graph and hypergraph theory that are required for our purpose. A *hypergraph* or *set system* F is a tuple $F := (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is a set of *vertices* and $\mathcal{E}$ is a family of subsets of $\mathcal{V}$. Sets of $\mathcal{E}$ are called *edges* of the hypergraph and cardinality of $\mathcal{E}$ is called *size* of the hypergraph; we will denote the size of F by $|\mathcal{E}|$. A hypergraph is called *simple* if it does not contain repeated edges, i.e., there are no multiple copies of any edge. A hypergraph is called *r-uniform* if each of its edges has cardinality r. A *graph* is a 2-uniform hypergraph. In most of the cases, we will consider simple graphs and hypergraphs only. So, by the terms graph and hypergraph we will refer to simple graphs and hypergraphs. We will use *multigraph* and *multihypergraph* to refer to graphs and hypergraphs with repeated edges.

Given a hypergraph $F = (\mathcal{V}, \mathcal{E})$, and a vertex $x \in \mathcal{V}$, *degree* of x, denoted as $deg_F(x)$, is the number of edges in $\mathcal{E}$ containing x; if there is no confusion regarding the hypergraph F, we will simply write it as $deg(x)$. Vertices $x, y \in \mathcal{V}$ are called *adjacent* if $\{x, y\} \subseteq E$ for some $E \in \mathcal{E}$. The *neighbourhood* of x, denoted as $\Gamma(x)$, is the set of all vertices adjacent to x, i.e., $\Gamma(x) = \{y \in \mathcal{V} | \{x, y\} \subseteq E \in \mathcal{E}\}$.

Also, given $\mathcal{U} \subseteq \mathcal{V}, \Gamma(\mathcal{U}) = \{y | y \in \Gamma(x) \text{ for some } x \in \mathcal{U}\}$, and expansion of $\mathcal{U}$ is given by $\frac{|\Gamma(\mathcal{U})|}{|\mathcal{U}|}$.

An r-uniform hypergraph $(\mathcal{V}, \mathcal{E})$ is called r-partite if its vertex set $\mathcal{V}$ can be partitioned into r classes $\mathcal{V}_1, \ldots, \mathcal{V}_r$ (i.e. $\mathcal{V} = \mathcal{V}_1 \cup \mathcal{V}_2 \cup \cdots \cup \mathcal{V}_r$ and $\mathcal{V}_i \cap \mathcal{V}_j = \emptyset$ for $i \neq j, 1 \leq i, j \leq r$), such that $\mathcal{E} \subseteq \mathcal{V}_1 \times \mathcal{V}_2 \times \ldots, \times \mathcal{V}_r$. The hypergraph is also denoted as $(\mathcal{V}_1, \ldots, \mathcal{V}_r, \mathcal{E})$. In particular, a graph $(\mathcal{L}, \mathcal{R}, \mathcal{E})$ is called *bipartite* if its set of vertices can be partitioned into two classes $\mathcal{L}$ and $\mathcal{R}$ such that $\mathcal{E} \subseteq \mathcal{L} \times \mathcal{R}$.

Further, by $K_n^{(r)}$ we will denote the complete r-uniform hypergraph $(\mathcal{V}, \mathcal{E})$ on n vertices, i.e., $\mathcal{E}$ is the set of all possible r-subsets of $\mathcal{V}$. By $K^{(r)}(\ell, \ldots, \ell)$ we will denote the complete r-uniform r-partite hypergraph $(\mathcal{V}_1, \ldots, \mathcal{V}_r, \mathcal{E})$ with ℓ vertices in each part, i.e., $|\mathcal{V}_i| = \ell$ for $1 \leq i \leq r$ and $\mathcal{E} = \mathcal{V}_1 \times \mathcal{V}_2 \times \ldots, \times \mathcal{V}_r$. We will denote by $K(s, t)$ the complete bipartite graph with partite sets of size s and t respectively. By C_i, we will denote a cycle of length i. For a graph with cycle, its *girth* is the length of the its shortest cycle.

Appendix B

Basics of Coding Theory

In this appendix, we recall basic details of coding theory. Part of the reason for this appendix is to provide necessary framework for Appendix C, where we give formal introduction to batch codes. Hence, the treatment of this appendix is slightly formal. We begin with definitions of a few technical terms.

– Alphabet: An alphabet Σ is a finite set of symbols. A very natural choice for Σ is the binary alphabet $\{0, 1\}$.

– Source: A source is a formal model of some natural phenomena such as human conversation, etc., which contains "information". More formally, a source $\mathscr{X} = \{X_i\}_{i \geq 1}$ is a sequence of discrete random variables. Here, we will assume that the variables X_i are independent with the same probability distribution $\mathcal{D}$ over the alphabet Σ. Such a source is called *discrete memoryless source*. So, for any $k \geq 1$, a discrete memoryless source naturally induces product distribution $\mathcal{D}^k$ on Σ^k, which is given by

$$\mathbf{Pr}\{X_1 \dots X_k = x_1 \dots x_k\} = \prod_{i=1}^{k} \mathbf{Pr}\{X_i = x_i\}, x_1, \dots, x_k \in \Sigma.$$

– Channel: A channel is a medium through which information is transmitted from source to destination. Formally, a channel $\mathscr{L} = (\Sigma, \Sigma, \mathbf{Pr}\{.|.\})$ is a tuple consisting of an input alphabet Σ, an output alphabet Σ, and transition probabilities $\mathbf{Pr}\{y|x\}$, where $\mathbf{Pr}\{y|x\}$ denotes the probability that the symbol $y \in \Sigma$ is received at the destination end of the channel given that $x \in \Sigma$ is sent at the source end. Similar to source, we assume the channel to be discrete memoryless as well. Hence, we have

$$\mathbf{Pr}\{y_1 \dots y_n | x_1 \dots x_n\} = \prod_{i=1}^{n} \mathbf{Pr}\{y_i | x_i\},$$

, where $y_1, \dots, y_n \in \Sigma$ are received in the destination end when $x_1, \dots, x_n \in \Sigma$ are sent at the source end. Here, we also assume that the channel characteristic is independent of the other parts of the system.

Purpose of *communication system* is to convey information from source (or sender), which generates information, to destination (or receiver) through a channel. The channel may be noisy, i.e., it may introduce error in the communication that alters the information sent. Here, we note that the source and the destination may be separated in time domain (in the case, where information is stored in a medium to be retrieved back at a later point in time, such as in a magnetic disk) or in space domain (in the case, where the information is transmitted from one place to another through a communication channel, such as in a wi-fi system). Since it is not possible to alter the characteristics of the source or channel, the way to achieve reliable and efficient (in terms of space, bandwidth, or time) communication is to transform the information in an appropriate manner.

Purpose of a *code* is to ensure reliability of communication through noisy channel in an efficient manner. Before proceeding further, we formally define a code and its associated parameters.

Definition B.1. A *code* C of length n over an alphabet Σ is a subset of Σ^n. Each member of C is called *codeword*. Given two codewords $c, c' \in C$, *distance* between c and c' is the number of places in which they differ, i.e., $dist(c, c') = |\{j \in [n] | c_j \neq c'_j\}|$. *Minimum distance* or simply *distance* d of C is defined as $d = dist(C) \triangleq \min_{c,c' c \neq c'} dist(c, c')$. *Rate* R of C is defined as $R \triangleq \frac{k}{n}$, where $k = \log_{|\Sigma|}|C|$.

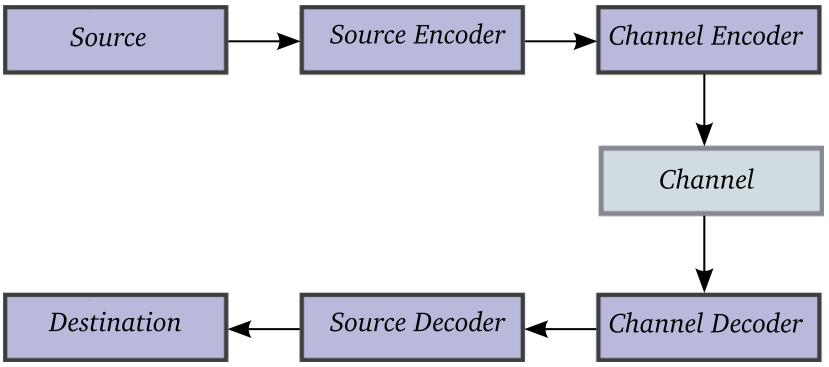

FIGURE B.1: *Communication System*

Associated with a code C are two mappings E and D. The mapping $E : \Sigma^k \mapsto \Sigma^n$, known as encoding, transforms a given message of length k into a codeword of length n. The mapping $D : \Sigma^n \mapsto \Sigma^k$, known as decoding, transform a codeword of lenth n into a message of length k.

Basic framework of a communication system is as follows. *Source encoder* transforms the raw information generated by the source into codewords of a suitably chosen *source code*. These codewords are then transformed by *channel encoder* into codewords of a suitably chosen *channel code* (or *error-correcting code*) for storage or transmission over the given medium. At the destination end, the received codewords are transformed back into original information using (consecutively) *channel decoder* and *source decoder* respectively. Next, we briefly elaborate on source code and channel code.

Source code: Loosely speaking, purpose of a source code is to capture information, generated by the source, into suitable form to make its storage and transmission possible through a given medium. In this case, the goal is to compress information in an efficient manner so that its transmission or storage requires less amount of bandwidth or space respectively. An important parameter of a source code C is *probability of decoding error*. For source $\mathscr{X}$, the probability of decoding error of the code C is given by

$$D_{err}(C, \mathscr{X}) \triangleq \underset{X^k \overset{\mathcal{D}^k}{\leftarrow} \Sigma^k}{\mathbf{Pr}} \{D(E(X^k)) \neq X^k\},$$

where $\mathcal{D}^k$ is the probability distribution on Σ^k according to which the source string X^k is generated.

Given source $\mathscr{X}$, the objective is to find a source code with high rate and low probability of decoding error. High rate ensures less space/ bandwidth for the transmitted information.[1]

Broadly speaking (and more precisely, for the error-free setting, i.e., in a setting where probability of decoding error is not allowed), source coding is concerned with the problem of minimizing storage / bandwidth in storing / transmitting information without considering the effect of the channel(noise). Hence, it is also called *noiseless coding*.

Channel code: Channel codes ensure reliable communication through a noisy medium. In this case, the goal is to encode the message word (i.e., the input word to the encoder) into a codeword in such a way so that message word can be recovered after decoding at the receiver, even if a significant portion of the transmitted codeword is corrupted by the channel noise. Analogous to source codes, for a channel $\mathscr{Z}$, the *average decoding error* of a (channel) code C is given by

$$D_{err}(C, \mathscr{Z}) \triangleq \frac{1}{|\Sigma|^k} \sum_{x_1 \dots x_k \in \Sigma^k} \mathbf{Pr}\{y_1 \dots y_n | E(x_1 \dots x_k)\} I(D(y_1 \dots y_n) \neq x_1 \dots x_k).$$

, where $\mathbf{Pr}(.|.)$ is the transition probability of the channel $\mathscr{Z}$ and $I(.)$ is the indicator function.

Similar to the case of source codes, for channel codes it is a challenging goal to find codes with low average decoding error and high rate. To this end, it can be observed that for a code with minimum distance d, it is always possible to recover the message word if the codeword is corrupted in at most $\lfloor \frac{d-1}{2} \rfloor$ positions. Hence, it is desirable to have codes with high rate and high minimum distance. In fact, formally stated, the prime goal, in this case, is construction of an infinite family $(n_i, k_i, d_i)_i$ binary codes with $\frac{k_i}{n_i} > 0$ and $\frac{d_i}{n_i} > 0$ together with efficient encoding and decoding algorithms.

[1]For source codes it is more natural to define the mappings E and D as $E : \Sigma^* \mapsto \Sigma^*, D : \Sigma^* \mapsto \Sigma^*$, i.e., from arbitrary length strings to arbitrary length strings. In fact, optimum codes like Huffman code are not block codes, but are of varying length. For simplicity, here, we defined them as block codes.

Appendix C

Brief Overview of Batch Codes

Purpose of this appendix is to provide an introduction to (general) batch codes in a more formal way, especially, to describe their practical motivation with some more detail. We begin with the formal definition of batch codes. Then we discuss multiset batch codes, which are important from practical perspective. Afterwards, we describe primitive batch codes, which capture underlying difficulty of the batch code problem. There, we also point out relationship of primitive batch codes with locally decodable codes. Finally, we discuss practical applications of batch codes. The material, presented in this appendix, is mostly from [IKOS04a], and it is not required for understanding our contribution (presented in Chapters 2-4).

Definition C.1 ***Batch code:*** *An (n, N, k, m, t)-batch code over an alphabet Σ is defined by an encoding function $C : \Sigma^n \rightarrow (\Sigma^*)^m$ (each output of which is called a bucket) and a decoding algorithm A such that*

(i) The total length of all m buckets is N (where the length of each bucket is independent of x);

(ii) For any $x \in \Sigma^n$ and $\{i_1, \ldots, i_k\} \subseteqq [n]$, $A(C(x), i_1, \ldots, i_k) = (x_{i_1}, \ldots, x_{i_k})$, and A probes at most t items from each bucket in $C(x)$ (whose positions are determined by $i_1, \ldots, i_k$).

Remark C.1. Definition of batch code does not specify the parameter k (which we termed "retrievability parameter" in Chapter 1) uniquely for a batch code. More precisely, an (n, N, k, m, t)-batch code is also an (n, N, k', m, t)-batch code for any $k' \leq k$. However, following the literature, we assume that it is the maximum possible k such that a decoding algorithm A can decode at most k items.

By (n, N, k, m)-batch code, we mean $(n, N, k, m, t = 1)$-batch code. Following corollary is immediate from the definition.

Corollary C.2 ([IKOS04a]). *1. An (n, N, k, m, t)-batch code (for any arbitrary t) implies an (n, tN, k, tm)-batch code.*

2. An (n, N, k, m)-batch code implies an (n, N, tk, m, t)-code and an $(n, N, k, \lceil \frac{m}{t} \rceil, t)$-code.

3. An (n, N, k, m)-batch code implies an (n, N, k, m)-code over $\Sigma = \{0, 1\}^w$, for an arbitrary w.

4. An (n, N, k, m)-batch code over $\{0, 1\}^w$ implies a (wn, wN, k, wm)-code over $\Sigma = \{0, 1\}$.

From the description given in Appendix B, it can be seen that batch codes, which are defined for a noiseless setting, can be classified as source codes. However, here the decoding is of certain type, which has some similarity with local decoding (to be discussed later). Like error-free source codes, one of the prime goals for batch codes is to find constructions with high rate, i.e., for given n constructions with minimum N.

Definition of batch codes does not limit the use of a retrieved item for decoding of multiple source items. However, in a multiuser scenario where users will try to decode source items parallelly, it is required that each retrieved data item be used for decoding only one source item. It is also possible that many users will try to decode the same source item. Motivated by this type of multiuser scenario the authors, in [IKOS04a], also defined *multiset batch codes*. The definition is stated for $t = 1$; however, it can be generalized for $t > 1$.

Definition C.2 ***Multiset batch code:*** *An (n, N, k, m)-multiset batch code is an (n, N, k, m)-batch code that satisfies the following additional properties. For any multiset $i_1, i_2, \ldots, i_k \in [n]$ there is a partition of the m buckets into subsets $S_1, S_2, \ldots, S_k \subseteq [m]$, such that each item x_{i_j}, $j \in [k]$, can be recovered by reading at most one item from each bucket in S_j.*

Example of a multiset batch code has been given in Example 1.1 of Chapter 1. In fact, that construction can be generalized for any value of m.

Another variant of batch codes, termed *primitive batch code*, captures inherent problem of batch codes in a more fundamental way. Next, we give its definition.

Definition C.3 ***Primitive batch code:*** *A primitive batch code is an (n, N, k, m)-batch code in which each bucket contains a single item, i.e., $N = m$.*

For primitive batch codes, always $t = 1$. We also note that primitive batch codes without multiset property are the trivial ones, i.e., each of the $m = n$ buckets contains a (distinct) source item. So, by primitive batch codes, we mean primitive multiset batch codes only. Since $N = m$ (and $t = 1$ automatically) for these codes, we write an (n, m, k, m)-primitive batch code as (n, k, m)-primitive batch code.

Example C.1 ***($\mathbf{n}, \mathbf{2}, \mathbf{n+1}$)-primitive batch code over $\{\mathbf{0}, \mathbf{1}\}$.*** A string $(x_1, \ldots, x_n)$ is encoded as $(x_1, \ldots, x_n, x_1 \oplus \cdots \oplus x_n)$. It follows (quite similar to Example 1.1 of Chapter 1) that any multiset of two source items can be decoded by reading from two disjoint sets of servers.

Few properties of multiset batch codes. Similar to error-correcting codes, multiset batch codes have the following properties, which we state without proofs.

Theorem C.3 (Direct product). *Let C_1 be an (n_1, N_1, k_1, m_1)-multiset batch code and C_2 be an (n_2, N_2, k_2, m_2)-batch code. Then there is an $(n_1 n_2, N_1 N_2, k, m_1 m_2)$-batch code, where $k \geq k_1 k_2$. Moreover, the code is multiset batch code if C_2 has multiset property.*

Theorem C.3 is essentially a direct product (between C_1 and C_2) construction. It is unification of Lemma 3.3 (Gadget lemma) and Lemma 3.5 (Composition lemma) of [IKOS04a] with a transparent view of the obtained parameters. However, its statement is more general in the sense that, in the composite construction of [IKOS04a] (obtained by unifying Lemma 3.3 (Gadget lemma) and Lemma 3.5 (Composition lemma)), it is required that C_1 be primitive, which is not the case for Theorem C.3. Indeed, C_1 can be an arbitrary (n_1, N_1, k_1, m_1)-multiset batch code. Proof of Theorem C.3 is given in [Bha14].

When a multiset batch code is viewed as a set of strings over some alphabet (arranged in buckets), we obtain the following lower bound on its minimum distance. Its proof is given in [IKOS04b].

Theorem C.4 (Distance). *Let C be any (n, N, k, m) multiset batch code having minimum distance d. Then $d \geq k$.*

Primitive batch codes also support concatenation. More specifically, we have the following theorem from [Bha14].

Theorem C.5 (Concatenation). *Let C_1 be an (n_1, k_1, m_1)-primitive mulitset batch code over alphabet Σ^{n_2} and C_2 be an (n_2, k_2, m_2)-primitive mulitset batch code over alphabet Σ, then there is an $(n_1 n_2, k_1 k_2, m_1 m_2)$-primitive multiset batch code over alphabet Σ, which is obtained by concatenating C_1 with C_2.*

In all the above three theorems, stated multiset properties are crucial; without it, the corresponding result will not hold. Now, we point out similarities and differences of primitive batch codes with locally decodable codes.

Relation with locally decodable codes (LDCs). Informally, an (r, δ, ϵ)-LDC over alphabet Σ is a mapping $C : \Sigma^k \mapsto \Sigma^n$, which maps a string $x \in \Sigma^k$ into a string $C(x) \in \Sigma^n$ so that the following holds. For any $i \in [k]$, the i-th item of x can be decoded by a randomized decoding algorithm with probability (taken over coin tosses of the randomized decoding algorithm) $\geq 1 - \epsilon$ by querying r items of $C(x)$, even if δn positions of $C(x)$ are corrupted.

LDCs were formally introduced in [KT00]. However, the basic idea and some of the techniques appeared earlier implicitly in the context of several other well studied problems such as self-correcting computations [GLR+91, GS92], random self-reducibility [AFK89, FF93, BF90], probabilistic checking of computations [BFLS91], worst-case to average-case reductions [BFNW93], private information retrieval [CKGS98], etc. Apart from many theoretical applications, LDCs are also important from practical perspective. In some practical scenarios, it is desirable to retrieve a small portion of the encoded message rather than the entire message efficiently (typically the decoding algorithm should be sublinear in the length of the codeword). One way to achieve this is by dividing the message into smaller blocks, and then encoding each block separately. However, such an encoding can not handle a constant fraction (of the codeword) of errors.

In order to compare LDCs with primitive batch codes, we note that both LDCs and primitive batch codes support local decoding in certain ways. In both cases, the objective is to decode parts of the input message instead of the whole message. Indeed, in case of LDCs, a particular symbol of the message, and in case of primitive batch codes, a set of k input message symbols are decoded.

However, there are fundamental differences between LDCs and primitive batch codes. LDCs support decoding from a corrupt (with a constant fraction corruption) codeword with a limited number of queries (this forces the decoding algorithm to be randomized). On the other hand, primitive batch codes support decoding from an error-free codeword with an unlimited number of queries (i.e., the whole codeword can be queried) in a restricted manner. Perhaps, due to this difference, there is a large gap between the lengths of the codewords in these cases. For example, a 2-query LDC require exponential length ([KdW04]); whereas, for an (n, k, m) primitive batch code it trivially follows that the length of the codeword $m \leq kn$.[1]

C.1 Application

C.1.1 Load balancing

Load balancing is inherent in the definition of batch codes. In fact, batch codes are abstraction of certain type of load balancing problem in coding theoretic terms. Broadly speaking, the goal of this load balancing problem is to store data items among a set of servers in such a way that a limited number of data items are retrieved from each server when a group of data items are retrieved. In this way, it is possible to limit maximum load on a particular server. Thus, no particular server is overloaded. This, in turn, ensures uniform availability of the participating servers.

With the advent of *cloud computing* (see [Gar11], [AFG+09]), a distributed computing paradigm that has fast emerged as a commercially successful state-of-the-art client-server computing model, it is reasonable to expect that these types

[1]Here, we stress that the two cases are not directly comparable owing to different types of restrictions in these two cases.

of codes will find practical applicability. One of the key concerns in cloud computing is to ensure availability of resources when needed (see [AFG+10]). Load balancing among resources, especially in a way so as not to overload a particular one, plays important role in maintaining availability and redundancy. It is in this scenario that batch codes, with their efficient encoding and decoding algorithms, can play very significant role.

C.1.2 Private information retrieval (PIR)

We consider the following problem: a user wants to retrieve a particular record from a public database without revealing the index of the retrieved record to the database. Here, the only concern is privacy of the index of the retrieved record, rather than privacy of the record or the privacy of the user. It is possible to solve the problem by sending the entire database to the user. This solution is clearly impractical as it requires huge communication overhead; namely, the whole database, which can be very large for practical applications.

This, however (see [CKGS98]), is the only solution (i.e., any other solution will require at least the same amount of communication overhead) if the database is stored in a single server, and the privacy requirement is information theoretic, i.e., if the server is assumed to be computationally unbounded. So, it is desirable to find better solutions by relaxing the assumptions in a feasible manner.

In [CKGS98], the authors proposed a construction for k-server PIR protocol. They consider the scenario where k identical copies of the database are stored in k servers, and the privacy requirement is that no server gets any information (in information theoretic sense) about the queried index. For a database of size n, this protocol requires $O(n^{\frac{1}{k}})$ communication. They also proposed a construction for 2-server PIR protocol that requires $O(n^{\frac{1}{3}})$ communication. More efficient constructions for k-server PIR protocol appeared in subsequent works [Amb97, BIKR02, BIK05, Ito99, Yek08, Efr12, KY09, CFL+13].

There have been different variations and extensions of this basic protocol. For example, the requirement of information theoretic privacy in the above protocol has been relaxed to computational privacy in [CG97, KO97], i.e., servers in protocols of [CG97, KO97] are assumed to be computationally polynomially (in the length of the database) bounded. For other variations and extensions and more recent results, see [Bei08, Gas04].

Mainstream research in PIR focused on reducing the communication complexity between user and server(s). This is because, in addition to being practically important, the goal has a certain theoretical appeal and well-established connection with other problems. However, another issue, which is no less important from practical point of view, is the (on-line) computational work done by server(s) in answering queries made by the user. In fact, in [SC07] (see also [OG12] for a more recent account of the practical issues of PIR), it was observed that computation time of the server(s) dominates the overall response time in answering a query made by the user. More precisely, the authors observed that the single server computational PIR protocol of [KO97], which involves computationally demanding number theory operations, is order of magnitude slower than the trivial protocol of sending the entire database; although communication complexity of the former is much less than the latter.

In every proposed solution of PIR protocol, it was observed that the computation on the part of database is at least linear in the length of the database. That it was not an artifact of proposed solutions, was first formally shown in [BIM04]. There, the authors have proven, *inter alia*, that for information theoretic privacy, expected total computational work done by the server(s) is at least linear in the length of the database. Following this, it was necessary to find alternative strategy to reduce on-line computation done by the servers, rather than finding ways to improve the protocols in terms of computational efficiency. Following alternatives were suggested and formally treated in the literature.

– *Auxiliary servers:* Delegate bulk of the on-line computation to auxiliary servers.

– *Preprocessing:* Preprocess database(s) before sending queries.

– *Amortization:* Amortize the computational work over multiple queries.

In [GGM98], the authors proposed a model that includes auxiliary (randomized) servers, in addition to the server that keeps the database. In their model, database is kept only in one server (database provider), and contents of the auxiliary servers can be made totally independent of the database. Given any PIR protocol, their model can bring down on-line computation of the database provider to $O(1)$ or no computation at all, while maintaining the privacy requirements of the original protocol. One advantage of their proposed solution is that replication of the original database is not needed for information theoretic security.

However, their solution hardly makes any progress in solving the original problem. Though on-line computation of the database provider is sufficiently reduced, on-line computation of the auxiliary servers remains same, i.e., linear in the size of the database. Communication complexity of their protocol is also higher than the communication complexity of the original protocol. Also, in order to achieve full information theoretic security, their proposed protocol requires costly resource of truly random bits that is linear in the size of the database. Their protocol also requires reinitialization, whose cost is linear in the length of the database, after a certain number of queries.

In the preprocessing based approach of [BIM04], proposed solutions include the following.

1. A k-server PIR protocol with $O(n^{1+\epsilon})$ extra storage, $O(\frac{n}{(\epsilon \log n)^{2k-2}})$ work, and $O(n^{\frac{1}{2k-1}})$ communication.
2. A k-server protocol with polynomially (in the size of the database) extra bits, and $O(n^{\frac{1}{k}+\epsilon})$ work and communication.

The proposed solutions reduce the amount of work done by the server(s) significantly. The solutions also provide a trade-off between extra storage and amount of work keeping the communication complexity same (in the first case), and between communication complexity and amount of work (in the second case). However, the requirement of extra storage, whose size is at least linear in the length of the database, seems prohibitive for large databases, where PIR is more likely to find application.

Amortization through batch codes. An (n, N, k, m)-batch code amortizes computational cost over k queries for an m-server PIR on a database of size n in the following manner. First the n-item database is encoded by the (n, N, k, m)-batch code. Let the amount of storage for the i-th bucket of the batch code be N_i, for $1 \leq i \leq m$. Hence, $\sum_{i=1}^{m} N_i = N$. Next, the i-th server stores the i-th bucket according to the requirement of a suitably chosen single server PIR protocol.

Now, on receiving k queries for the original n-item database, the batch decoder generates a single query for each server. Next, each server runs the chosen single server PIR protocol for its query on its database, and returns the corresponding data item(s). Finally, the batch decoder outputs k queried items from the items

returned by the m servers. Total computational overhead for the servers in this case is $\sum_{i=1}^{m} T(N_i)$ and communication overhead is $\sum_{i=1}^{m} C(N_i)$, where $T(N_i)$ and $C(N_i)$ are the computational and communication cost of PIR protocols for the i-th server on a database of size N_i.

First, we note that the above protocol is correct and secure if the underlying single server protocol is so. Now, significant saving in computational and communication cost may be achieved if $\sum_{i=1}^{m} T(N_i)$ and $\sum_{i=1}^{m} C(N_i)$ are significantly less than kn. For example, in a theoretical setting, this can already be achieved by using the $(n, 2, n+1)$-primitive batch code of Example C.1.

Bibliography I

[AFK89] M. Abadi, J. Feigenbaum, and J Kilian. On hiding information form an oracle. *J. Comput. Syst. Sci.*, 39(1):21–50, August 1989.

[AVZ00] Erik Agrell, Alexander Vardy, and Kenneth Zeger. Upper bounds for constant-weight codes. *IEEE Transactions on Information Theory*, 46(7):2373–2395, 2000.

[AS00] N Alon and JH Spencer. *The Probabilistic Method*. Wiley-Interscience, New York, 2nd edition, 2000.

[ABI86] Noga Alon, Laszlo Babai, and Alon Itai. A fast and simple randomized parallel algorithm for the maximal independent set problem. *Journal of Algorithms*, 7(4):567 – 583, 1986.

[Amb97] Andris Ambainis. Upper bound on the communication complexity of private information retrieval. In Pierpaolo Degano, Roberto Gorrieri, and Alberto Marchetti-Spaccamela, editors, *Proceedings of the 24th International Colloquium on Automata, Languages and Programming*, volume 1256 of *Lecture Notes in Computer Science*, pages 401–407. Springer Berlin Heidelberg, 1997.

[AFG+10] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. A view of cloud computing. *Commun. ACM*, 53(4):50–58, April 2010.

[AFG+09] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, and Matei Zaharia. Above the clouds: A berkeley view of cloud computing. Technical report, University of California at Berkeley, 2009.

[BFLS91] László Babai, Lance Fortnow, Leonid A. Levin, and Mario Szegedy. Checking computations in polylogarithmic time. In *Proceedings of the Twenty-third Annual ACM Symposium on Theory of Computing*, STOC '91, pages 21–32, New York, NY, USA, 1991. ACM.

[BFNW93] László Babai, Lance Fortnow, Noam Nisan, and Avi Wigderson. Bpp has subexponential time simulations unless exptime has publishable proofs. *Comput. Complex.*, 3(4):307–318, October 1993.

[BT11] Rahil Baber and John Talbot. Hypergraphs do jump. *Combinatorics, Probability and Computing*, 20:161–171, 3 2011.

[BB14] Niranjan Balachandran and Srimanta Bhattacharya. On an extremal hypergraph problem related to combinatorial batch codes. *Discrete Applied Mathematics*, 162:373–380, 2014.

[BF90] Donald Beaver and Joan Feigenbaum. Hiding instances in multioracle queries. In Christian Choffrut and Thomas Lengauer, editors, *STACS 90*, volume 415 of *Lecture Notes in Computer Science*, pages 37–48. Springer Berlin Heidelberg, 1990.

[Bei08] Amos Beimel. Private information retrieval: A primer. 2008.

[BIK05] Amos Beimel, Yuval Ishai, and Eyal Kushilevitz. General constructions for information-theoretic private information retrieval. *Journal of Computer and System Sciences*, 71(2):213–247, 2005.

[BIKR02] Amos Beimel, Yuval Ishai, Eyal Kushilevitz, and J-F Raymond. Breaking the $o(n^{\frac{1}{(2k-1}})$ barrier for information-theoretic private information retrieval. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002.*, pages 261–270. IEEE, 2002.

[BIM04] Amos Beimel, Yuval Ishai, and Tal Malkin. Reducing the servers' computation in private information retrieval: Pir with preprocessing. *Journal of Cryptology*, 17(2):125–151, March 2004.

[BR94] M. Bellare and J. Rompel. Randomness-efficient oblivious sampling. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS'94)*, pages 276–287, Washington, DC, USA, 1994. IEEE Computer Society.

[BAS14] Avraham Ben-Aroya and Igor Shinkar. A note on subspace evasive sets. *Chicago Journal of Theoretical Computer Science*, 2014(9), November 2014.

[BR91] Bonnie Berger and John Rompel. Simulating ($\log^c n$)-wise independence in nc. *J. ACM*, 38(4):1026–1046, October 1991. Preliminary version in Proceedings of the 30th Annual Symposium on Foundations of Computer Science (FOCS'89).

[Bha14] Srimanta Bhattacharya. Batch codes revisited, 2014.

[Bha15] Srimanta Bhattacharya. Derandomized construction of combinatorial batch codes. In Adrian Kosowski and Igor Walukiewicz, editors, *Fundamentals of Computation Theory - 20th International Symposium, FCT 2015, Gdańsk, Poland, August 17-19, 2015, Proceedings*, volume 9210 of *Lecture Notes in Computer Science*, pages 269–282. Springer, 2015.

[BRR12] Srimanta Bhattacharya, Sushmita Ruj, and Bimal K. Roy. Combinatorial batch codes: A lower bound and optimal constructions. *Adv. in Math. of Comm.*, 6(2):165–174, 2012.

[BS15] Srimanta Bhattacharya and Sumanta Sarkar. On some permutation binomials and trinomials over $\mathbb{F}_{2^n}$. In *The Ninth International Workshop on Coding and Cryptography (WCC) 2015*, 2015.

[Bol78] Béla Bollobás. *Extremal Graph Theory*. Dover, New York, 1978.

[Bol86] Béla Bollobás. *Combinatorics: set systems, hypergraphs, families of vectors, and combinatorial probability*. Cambridge University Press, 1986.

[Bol98] Béla Bollobás. *Modern Graph Theory*. Graduate Texts in Mathematics 184. Springer, New York, 1998.

[BS74] J. A. Bondy and M. Simonovits. Cycles of even length in graphs. *Journal of Combinatorial Theory, Series B*, 16(2):97 – 105, 1974.

[BE10] Andries E Brouwer and Tuvi Etzion. Some new distance-4 constant weight codes, 2010.

[BSSS90] Andries E Brouwer, James B Shearer, Neil JA Sloane, and Warren D Smith. A new table of constant weight codes. *IEEE Transactions on Information Theory*, 36(6):1334–1380, 1990.

[BES73] W. G. Brown, P. Erdős, and V. T. Sós. Some extremal problems on r-graphs. In New directions in the theory of graphs, *Proc. third conference on graph theory at Ann Arbor*, pages 53 – 63, 1973.

[BKMS10a] Richard A. Brualdi, Kathleen Kiernan, Seth A. Meyer, and Michael W. Schroeder. Combinatorial batch codes and transversal matroids. *Adv. in Math. of Comm.*, 4(3):419–431, 2010.

[BKMS10b] Richard A. Brualdi, Kathleen Kiernan, Seth A. Meyer, and

Michael W. Schroeder. Erratum. *Adv. in Math. of Comm.*, 4(4):597, 2010.

[Bsh15] NaderH. Bshouty. Linear time constructions of some d-restriction problems. In Vangelis Th. Paschos and Peter Widmayer, editors, *Algorithms and Complexity*, volume 9079 of *Lecture Notes in Computer Science*, pages 74–88. Springer International Publishing, 2015.

[BMRV02] Harry Buhrman, Peter Bro Miltersen, Jaikumar Radhakrishnan, and Srinivasan Venkatesh. Are bitvectors optimal? *SIAM J. Comput.*, 31(6):1723–1744, 2002.

[BT11a] Cs. Bujtás and Zs. Tuza. Optimal combinatorial batch codes derived from dual systems. *Miskolc Mathematical Notes*, 12(4):11–23, 2011.

[BT11b] Csilla Bujtás and Zsolt Tuza. Combinatorial batch codes: Extremal problems under hall-type conditions. *Electronic Notes in Discrete Mathematics*, 38:201–206, 2011.

[BT11c] Csilla Bujtás and Zsolt Tuza. Optimal batch codes: Many items or low retrieval requirement. *Adv. in Math. of Comm.*, 5(3):529–541, 2011.

[BT12] Csilla Bujtás and Zsolt Tuza. Relaxations of hall's condition: Optimal batch codes with multiple queries. *Appl. Anal Discrete Math.*, 6:72–81, 2012.

[BT15] Csilla Bujtás and Zsolt Tuza. Turán numbers and batch codes. *Discrete Applied Mathematics*, 186:45 – 55, 2015.

[Cae83] D. De Caen. Extension of a theorem of Moon and Moser on complete subgraphs. *Ars Combinatoria*, pages 5–10, 1983.

[CFL+13] Yeow Meng Chee, Tao Feng, San Ling, Huaxiong Wang, and Liang Feng Zhang. Query-efficient locally decodable codes of subexponential length. *Computational Complexity*, pages 1–31, 2013.

[CG97] Benny Chor and Niv Gilboa. Computationally private information retrieval. In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pages 304–313. ACM, 1997.

[CKGS98] Benny Chor, Eyal Kushilevitz, Oded Goldreich, and Madhu Sudan. Private information retrieval. *Journal of the ACM (JACM)*, 45(6):965–981, 1998.

[Efr12] Klim Efremenko. 3-query locally decodable codes of subexponential length. *SIAM Journal on Computing*, 41(6):1694–1703, 2012.

[Erd64] P. Erdős. On extremal problems of graphs and generalized graphs. *Israel Journal of Mathematics*, 2(3):183–190, 1964.

[Erd71] P. Erdős. On some extremal problems on r-graphs. *Discrete Mathematics*, 1(1):1 – 6, 1971.

[ERS66] P. Erdős, A. Rényi, and V. T. Sós. On extremal problems of graphs and generalized graphs. *Stud. Sci. Math. Hung.*, 1:215–235, 1966.

[ES73] P Erdős and J.L Selfridge. On a combinatorial game. *Journal of Combinatorial Theory, Series A*, 14(3):298 – 301, 1973.

[ES66] P. Erdős and M. Simonovits. A limit theorem in graph theory. *Stud. Sci. Math. Hungar.*, 1:51–57, 1966.

[ES46] P. Erdős and A. H. Stone. On the structure of linear graphs. *Bull. Amer. Math. Soc.*, 52(12):1087–1091, 12 1946.

[FS83] RalphJ. Faudree and Miklós Simonovits. On a class of degenerate extremal graph problems. *Combinatorica*, 3(1):83–93, 1983.

[FF93] J. Feigenbaum and L. Fortnow. Random-self-reducibility of complete sets. *SIAM Journal on Computing*, 22(5):994–1005, 1993.

[FF84] Peter Frankl and Zoltán Füredi. An exact result for 3-graphs. *Discrete Mathematics*, 50:323–328, 1984.

[FS13] Z Füredi and M Simonovits. The history of degenerate (bipartite) extremal graph problems. 25:167–262, 2013.

[Fűr91] Zoltán Fűredi. Turán type problems. *Surveys in combinatorics, London Math. Soc. Lecture Note Ser*, 166:253–300, 1991.

[Gar11] Simson Garfinkel. The cloud imperative. `http://www.technologyreview.com/news/425623/the-cloud-imperative/`, 2011. Retrieved 26th November, 2013.

[Gas04] William Gasarch. A survey on private information retrieval. In *Bulletin of the EATCS*, 2004.

[GLR+91] Peter Gemmell, Richard Lipton, Ronitt Rubinfeld, Madhu Sudan, and Avi Wigderson. Self-testing/correcting for polynomials and for approximate functions. In *Proceedings of the Twenty-third Annual ACM Symposium on Theory of Computing*, STOC '91, pages 33–42, New York, NY, USA, 1991. ACM.

[GS92] Peter Gemmell and Madhu Sudan. Highly resilient correctors for polynomials. *Inf. Process. Lett.*, 43(4):169–174, September 1992.

[GGM98] Yael Gertner, Shafi Goldwasser, and Tal Malkin. A random server

model for private information retrieval or how to achieve information theoretic pir avoiding database replication. In *RANDOM*, pages 200–217, 1998.

[GS80] R Graham and N Sloane. Lower bounds for constant weight codes. *IEEE Transactions on Information Theory*, 26(1):37–43, 1980.

[GUV09] Venkatesan Guruswami, Christopher Umans, and Salil Vadhan. Unbalanced expanders and randomness extractors from parvaresh–vardy codes. *J. ACM*, 56(4):20:1–20:34, July 2009. Preliminary version in Proceedings of the Twenty-Second Annual IEEE Conference on Computational Complexity (CCC '07).

[Hoe63] Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301):pp. 13–30, 1963.

[HLW06] Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *Bull. Amer. Math. Soc. (N.S*, 43:439–561, 2006.

[IKOS04a] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Batch codes and their applications. In László Babai, editor, *Proceedings of the 36th Annual ACM Symposium on Theory of Computing, Chicago, IL, USA, June 13-16, 2004*, pages 262–271. ACM, 2004.

[IKOS04b] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Batch codes and their applications. In László Babai, editor, *Proceedings of the 36th Annual ACM Symposium on Theory of Computing, Chicago, IL, USA, June 13-16, 2004 (Submitted Version)*, pages 262–271. ACM, 2004.

[Ito99] Toshiya Itoh. Efficient private information retrieval. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 82(1):11–20, 1999.

[KNS64] GOH Katona, T Nemetz, and M Simonovits. On a graph-problem of turán in the theory of graphs. *Journal title Matematikai Lapok*, pages 228–238, 1964.

[KT00] Jonathan Katz and Luca Trevisan. On the efficiency of local decoding procedures for error-correcting codes. In *Proceedings of the Thirty-second Annual ACM Symposium on Theory of Computing*, STOC '00, pages 80–86, New York, NY, USA, 2000. ACM.

[KY09] Kiran S Kedlaya and Sergey Yekhanin. Locally decodable codes

from nice subsets of finite fields and prime factors of mersenne numbers. *SIAM Journal on Computing*, 38(5):1952–1969, 2009.

[Kee11] P Keevash. Hypergraph turán problems. *Surveys in Combinatorics*, pages 83–140, 2011.

[KdW04] Iordanis Kerenidis and Ronald de Wolf. Exponential lower bound for 2-query locally decodable codes via a quantum argument. *Journal of Computer and System Sciences*, 69(3):395 – 420, 2004. Special Issue on {STOC} 2003.

[Klo81] Torliev Klove. Lower bound for $a(n, 4, w)$. *IEEE Transactions on Information Theory*, 27(2):257–258, 1981.

[KST54] P. Kővári, V. T. Sós, and P. Turán. On a problem of k. zarankiewicz. *Colloquium Mathematicum*, 3:50–57, 1954.

[KO97] Eyal Kushilevitz and Rafail Ostrovsky. Replication is not needed: Single database, computationally-private information retrieval. In *Proceedings of the 38th Annual Symposium on Foundations of Computer Science, 1997.*, pages 364–373. IEEE, 1997.

[LUW95] Felix Lazebnik, Vasiliy A Ustimenko, and Andrew J Woldar. A new series of dense graphs of high girth. *Bulletin of the American Mathematical Society*, 32(1):73–79, 1995.

[Man07] W Mantel. Problem 28. *Wiskundige Opgaven*, 10:60–61, 1907.

[MNN94] Rajeev Motwani, Joseph (Seffi) Naor, and Moni Naor. The probabilistic method yields deterministic parallel algorithms. *Journal of Computer and System Sciences*, 49(3):478 – 516, 1994. Preliminary version in Proceedings of the 30th Annual Symposium on Foundations of Computer Science (FOCS'89).

[MR95] Rajeev Motwani and Prabhakar Raghavan. *Randomized Algorithms*. Cambridge University Press, New York, NY, USA, 1995.

[Mub03] Dhruv Mubayi. On hypergraphs with every four points spanning at most two triples. *Electr. J. Comb.*, 10, 2003.

[Mub12] Dhruv Mubayi. personal communication, 2012.

[MT08] Dhruv Mubayi and John M. Talbot. Extremal problems for t-partite and t-colorable hypergraphs. *Electr. J. Comb.*, 15(1), 2008.

[NSS95] M. Naor, L. J. Schulman, and A. Srinivasan. Splitters and near-optimal derandomization. In *Proceedings of the 36th Annual Symposium on Foundations of Computer Science*, FOCS '95, pages 182–, Washington, DC, USA, 1995. IEEE Computer Society.

[OG12] Femi Olumofin and Ian Goldberg. Revisiting the computational practicality of private information retrieval. In *Proceedings of the 15th International Conference on Financial Cryptography and Data Security*, FC'11, pages 158–172, Berlin, Heidelberg, 2012. Springer-Verlag.

[PSW09] Maura B Paterson, D Stinson, and R Wei. Combinatorial batch codes. *Advances in Mathematics of Communications*, 3(1):13–27, 2009.

[PT09] Stanley E Payne and J Joseph Adolf Thas. *Finite generalized quadrangles*, volume 110. European Mathematical Society, 2009.

[Pik12] Oleg Pikhurko. A note on the turán function of even cycles. *Proceedings of the American Mathematical Society*, 140(11):3687–3692, 2012.

[PR04] Pavel Pudlák and Vojtech Rödl. Pseudorandom sets and explicit constructions of ramsey graphs. *Quaderni di Matematica*, 13:327–346, 2004.

[Rab89] Michael Rabin. Efficient dispersal of information for security, load balancing, and fault tolerance. *Journal of the ACM*, 36:335–348, 1989.

[RTS00] Jaikumar Radhakrishnan and Amnon Ta-Shma. Bounds for dispersers, extractors, and depth-two superconcentrators. *SIAM J. Discret. Math.*, 13(1):2–24, January 2000.

[Rag88] Prabhakar Raghavan. Probabilistic construction of deterministic algorithms: Approximating packing integer programs. *J. Comput. Syst. Sci.*, 37(2):130–143, October 1988.

[Raz07] Alexander A. Razborov. Flag algebras. *Journal of Symbolic Logic*, 72(4):1239–1282, 12 2007.

[Raz10] Alexander A. Razborov. On 3-hypergraphs with forbidden 4-vertex configurations. *SIAM J. Discret. Math.*, 24(3):946–963, August 2010.

[SBÇ12] Sumanta Sarkar, Srimanta Bhattacharya, and Ayça Çesmelioglu. On some permutation binomials of the form $x^{\frac{2^n-1}{k}+1} + ax$ over $\mathbb{F}_{2^n}$: Existence and count. In *Arithmetic of Finite Fields - 4th International Workshop, WAIFI 2012, Bochum, Germany, July 16-19, 2012. Proceedings*, pages 236–246, 2012.

[Sid95] Alexander Sidorenko. What we know and what we do not know about turán numbers. *Graphs and Combinatorics*, 11(2):179–199, 1995.

[SG14] Natalia Silberstein and Anna Gál. Optimal combinatorial batch codes based on block designs. *Designs, Codes and Cryptography*, pages 1–16, 2014.

[SC07] Radu Sion and Bogdan Carbunar. On the computational practicality of private information retrieval. In *In Proceedings of the Network and Distributed Systems Security Symposium, 2007. Stony Brook Network Security and Applied Cryptography Lab Tech Report*, 2007.

[SS96] Michael Sipser and Daniel A. Spielman. Expander codes. *IEEE Transactions on Information Theory*, 42(6):1710–1722, 1996.

[SHP06] Derek H Smith, Lesley A Hughes, and Stephanie Perkins. A new table of constant weight codes of length greater than 28. *Electron. J. Combin*, 13(1):18, 2006.

[Spe94] J. Spencer. *Ten Lectures on the Probabilistic Method*. Society for Industrial and Applied Mathematics, 2nd edition, 1994.

[Sud10] Benny Sudakov. Recent developments in extremal combinatorics: Ramsey and turán type problems. In *Proceedings of The International Congress of Mathematicians, Hyderabad, India*, pages 2579–2606. World Scientific, 2010.

[Tal07] John Talbot. Chromatic turán problems and a new upper bound for the turán density of k4-. *Eur. J. Comb.*, 28(8):2125–2142, November 2007.

[Tur41] Paul Turán. On an extremal problem in graph theory (in hungarian). *Mat. Fiz. Lapok*, 48:436–452, 1941.

[VPE89] Cornelis LM Van Pul and Tuvi Etzion. New lower bounds for constant weight codes. *IEEE Transactions on Information Theory*, 35(6):1324–1329, 1989.

[Ver00] Jacques Verstraëte. On arithmetic progressions of cycle lengths in graphs. *Combinatorics, Probability and Computing*, 9(04):369–373, 2000.

[Yek08] Sergey Yekhanin. Towards 3-query locally decodable codes of subexponential length. *Journal of the ACM (JACM)*, 55(1):1, 2008.

Part II

On Some Cyclotomic Mapping Permutation Binomials Over $\mathbb{F}_{2^n}$

Notation Summary For Chapter 5 and Appendix D

Here, we formally state our notational convention for this part of the thesis.

1. Lower case Greek letters will denote field elements.
2. Upper case Roman letters will denote sets as well as special functions.
3. Among lower case Roman letters
   (a) $\{a, b, c\}$ will denote field elements, this choice is guided by common practice in the literature;
   (b) $\{d, e\}$ will denote integers;
   (c) $\{f, g, h\}$ will denote functions;
   (d) $\{i, j, k, \ell, m, n, o, p, q, r, s, t, u, v, w\}$ will denote integers with $\{i, j\}$ normally reserved for indices and $\{p, q\}$ reserved for prime and prime power respectively;
   (e) $\{x, y, z\}$ will denote variables and indeterminates.
4. Conventions on asymptotic notations $O(.)$ and $\Omega(.)$ remains same as in the first part.

Chapter 5

On Some Cyclotomic Mapping Permutation Binomials Over $\mathbb{F}_{2^n}$

5.1 Introduction

In this chapter, we study *permutation binomials* (PBs) of the form $x^{\frac{2^n-1}{2^t-1}+1} + ax$ over $\mathbb{F}_{2^n}$. We explicitly characterize and enumerate these PBs under certain restrictions. These PBs belong to the class of *cyclotomic mapping polynomials* (definitions and details to be discussed later). Also, these PBs are very closely related to *orthomorphisms / complete mappings*, which are special types of permutations with applications in constructions of various combinatorial designs.

Permutation polynomials (PPs) over finite fields have a long and rich history. In order to set the context for our results, in Section 5.1, we give an overview of basic problems and results of this area that are relevant to our work. This also includes brief discussion on cyclotomic mapping polynomials and orthomorphisms. In section 5.2, we discuss our contribution as well as existing results which are more specific to our contribution. In Section 5.3, we provide proofs of our results. Finally, we conclude in Section 5.4

5.1.1 BACKGROUND AND MOTIVATION

It is well known that finite fields are *polynomially complete*, i.e., any function mapping a finite field to itself can be represented by a polynomial.[1] PPs are those polynomials that induce a permutation function. More formally, we have:

Definition 5.1. Let $\mathbb{F}_q$ be a finite field of q elements. A polynomial $f \in \mathbb{F}_q[x]$ is a PP of $\mathbb{F}_q$ if the function $\mathbf{f} : a \mapsto f(a), a \in \mathbb{F}_q$, is a permutation of $\mathbb{F}_q$.

Following are some well-known classes of PPs.

Example 5.1. (*i*) *Monomials:* x^d is a PP of $\mathbb{F}_q$ iff $\gcd(d, q-1) = 1$.

(*ii*) *Linearized polynomials:* A polynomial of the form $L(x) = \sum_{s=0}^{n-1} a_s x^{q^s} \in \mathbb{F}_q[x]$ is a PP of $\mathbb{F}_q$ *iff* $L(x) = 0 \implies x = 0$.

(*iii*) *Dickson polynomials:* For $a \in \mathbb{F}_q$, $k \in \mathbb{N}$, and indeterminate x, *Dickson polynomial* of the first kind [2] $D_k(x, a)$ is defined as

$$D_k(x, a) = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-a)^j x^{k-2j}$$

It is known that the Dickson polynomial $D_k(x, a), a \in \mathbb{F}_q^*$, is a permutation polynomial of $\mathbb{F}_q$ if and only if $\gcd(k, q^2 - 1) = 1$

Study of PPs can be traced back to the work of Betti ([Bet51, Bet55]), Mathieu ([Mat61]), Hermite ([Her63]), Brioschi ([Bri70, Bri79]), Grandi ([Gra81, Gra83]). Perhaps the first systematic exposition on the topic is the seminal work of Dickson [Dic96] (arising out in connection with his work on linear groups([Dic58])). Since then PPs have been subject of extensive research; a rigorous account of this can be found in [LN97]. Selected aspects of the early part of the development of the theory have also been captured in [LN73, Sma91]. Several open problems that were outcome of the early part of the development, were formally discussed in [LM88, LM93].

[1] In fact, finite field is the only algebraic structure possessing this property. Given a function $\mathbf{f} : \mathbb{F}_q \mapsto \mathbb{F}_q$, the unique polynomial $f(x) \in \mathbb{F}_q[x]$ representing $\mathbf{f}$ is given by $f(x) = \sum_{a \in \mathbb{F}_q} \mathbf{f}(a)(1 - (x-a)^{q-1})$.

[2] See [LN97, LMT93] for details on this interesting class of polynomials.

PPs represent purely combinatorial constructs, namely permutations. This influences their algebraic attributes. For example (formally stated as Corollary 5.5), for $d \mid q-1$, there are no PP of degree d over $\mathbb{F}_q$. Also, it is known (and formally proven in [Das02, KP02]) that almost all PPs over $\mathbb{F}_q$ have degree $q-2$. On the other hand, many outstanding problems of the theory, such as Carlitz's conjecture on exceptional polynomials (PPs that permute infinitely many extensions of a finite field), require deep algebraic machinery for their resolution. This interplay between combinatorics and algebra makes PPs theoretically appealing.

PPs over finite fields, especially over prime fields are theoretically very important as well. For example, it can be shown (see [Nar84, Nöb65]) (by Chinese Remainder Theorem) that permutation behaviour of a polynomial f modulo an integer n is essentially determined by permutation behaviours of f over $\mathbb{F}_{p_i}$ s (with some additional conditions), where the prime power decomposition of n is given by $n = \prod_i p_i^{a_i}$.

While the above facts underlie broad theoretical appeal and importance for study of PPs over finite fields, it is perhaps the concrete problems of this theory that generated significant interest among researchers. Problems such as characterization, existence and enumeration, algorithmic testing, investigation of group structure generated by various classes of PPs, etc. have received significant attention in the literature. In this thesis, we consider two problems of fundamental importance - (*i*) characterization, and (*ii*) existence and enumeration of PPs. Next, we present a brief outline of these two categories of problems.[3]

Characterization. Finding necessary and sufficient conditions for a class of polynomials to be PPs forms the crux of research on PPs. We term a class of PPs *characterized* if there are necessary and sufficient conditions (to be PP) for polynomials belonging to that class. A trivial characterization for the class of all PPs (arising out of the definition of PPs) is that the cardinality of the value set[4] of a polynomial over $\mathbb{F}_q$ is q iff it is a PP. The first non-trivial characterization for the class of all PPs is given by the following result, commonly known as Hermite-Dickson criteria. Hermite ([Her63]) formulated the criteria for prime fields, Dickson ([Dic96]) extended it to non-prime fields. We will use this criteria later to prove Theorem 5.2.2.

[3]For a detailed account of results related to various other problems see notes (though slightly dated) at the end of Chapter 7 of [LN97]. For results related to algorithmic testing of PPs see [Shp92b, MvzG94, MVZG95b, MVZG95a, Kay05].

[4]For a polynomial $f \in \mathbb{F}_q[x]$, its value set is the set $\{f(a) : a \in \mathbb{F}_q\}$.

Theorem 5.2 ([LN97]). *A polynomial $f \in \mathbb{F}_q[x]$ is a PP if and only if*

(i) *f has exactly one root in $\mathbb{F}_q$,*

(ii) *$f^t \mod (x^q - x)$ has degree less than $q-1$ for $1 \leq t \leq q-2, p \nmid t$, where p is the characteristic of $\mathbb{F}_q$.*

Remark 5.3. In the above theorem the condition $p \nmid t$ can be removed; in fact, we will do so in the proof of Theorem 5.2.2.

Alternate characterization for the class of all PPs have been proposed in the literature (see [LZ67, Vau74, Wan92, Tur95]). For example, in [Wan92], the author characterized PPs in terms of value sets, and in [Tur95], the author extended this approach in various directions. Another very useful characterization can be given in terms of *additive characters*; see [LN97] for details.

Here, we point out an important aspect of characterization of PPs in terms of computational complexity of evaluating the necessary and sufficient conditions that describe the characterization. First, we note that a finite field of q elements can be represented on a machine (or more formally on a RAM) using $O(\log q)$ bits. Runtime of an algorithm involving operations of a finite field of q elements is measured in terms of the size of the representation of the field, which is $O(\log q)$.[5] An algorithms whose runtime is bounded by a polynomial in $\log q$, i.e., runtime is $poly(\log q)$, is practically feasible. We term this algorithm *efficient*. For example, there are efficient algorithms to check necessary and sufficient conditions of all the classes of PPs discussed in Example 5.1. For example, in case of Example 5.1 (i) computing the gcd takes time $O((\log q)^3)$. However, this does not seem to be the case for the necessary and sufficient conditions of Theorem 5.2 (and in general for the other characterizations of the class of all PPs discussed above). It can only be guaranteed that these conditions can be evaluated in time $O(q)$, which is exponential in $\log q$; and hence, are not efficient. This motivates us to formally introduce the notion of explicit characterization of a class of PPs.

[5]It is possible that the algorithm takes several inputs. In that case, the runtime becomes a function of the sizes of all inputs. However, more frequently, these additional inputs turn out to be constant parameters and they do not affect the asymptotic runtime of the algorithm. More specifically, these additional constant parameters do not affect the polynomiality (in terms of $\log q$) of the runtime.

Definition 5.4. A class of PPs over $\mathbb{F}_q$ is *explicitly characterized* if there are necessary and sufficient conditions for the class which can be checked efficiently for each polynomial belonging to the class; i.e., if the conditions can be checked by a deterministic algorithm which given as input a representation of $\mathbb{F}_q$ and expression for any polynomial belonging to the class in the given representation, runs in time polynomial in $\log q$ and in the (binary) length of the parameters (which are independent of q) defining the class.

For example, an explicit characterization of the class of PPs of the form $x^r f(x^{\frac{q-1}{d}})$, where d, r are parameters independent of q, would comprise of necessary and sufficient conditions that can be checked by an algorithm that runs in time $poly(\log q, \log d, \log r)$. Without providing details, we mention that the characterizations in Example 5.1 can be evaluated efficiently (see [vzGG13, Shp92a] for algorithmic aspects of finite fields). Hence, classes of PPs in Example 5.1 are explicitly characterized.

However, it is not known whether the class of all PPs can be explicitly characterized.[6] So, a reasonable goal is to obtain explicit characterization of specific classes of PPs. While the monomials are explicitly characterized (Example 5.1(a)), there is no such explicit characterization for binomials in general. So, characterization of binomials is the "next" non-trivial open case. Hence, for a systematic understanding of characterization of PPs it is highly desirable to characterize binomials, or at least specific classes of binomials.

Existence and enumeration. Characterization brings forth the question of existence and enumeration of specific classes of PPs, which form some of the most fundamental open problems. For example, the characterization of monomials given in Example 5.1(a) immediately implies that the number of permutation monomials is $(q-1)\phi(q-1)$, where $\phi(.)$ is the Euler's phi function. On the other hand, Hermite-Dickson criteria (Theorem 5.2) implies the following general non-existence result.

[6] In [Kay05], the author gave a deterministic algorithm to test PPs of degree ℓ that runs in time $poly(\ell \log q)$. This leads to explicit characterization of the class of PPs with degree $\ell = poly(\log q)$. However, the algorithm is not useful when ℓ is superpolynomial in $\log q$ (as the runtime of the algorithm becomes superpolynomial in $\log q$, and hence the algorithm is not efficient for these values of ℓ). The polynomials considered in this work are of the form $x^r f(x^{\frac{q-1}{d}})$, where r is constant and $d = O(\sqrt{q})$, so they have degree superpolynomial in $\log q$. Hence, the algorithm of [Kay05] is not relevant to our case.

Corollary 5.5 (of Theorem 5.2)**.** *If $d > 1$ is divisor of $q-1$ then there is no PP of $\mathbb{F}_q$ of degree d.*

Several other non-existence results (see, e.g., [Wan87, Tur88, MZ09]), especially for PPs over prime fields were proven using Hermite-Dickson criteria.

However, these questions, in general, often require rather deep tools from algebra and geometry for their resolution. One such important example of wide generality is the Carlitz-Wan conjecture, which is now a proven result (see [Wan93, CF95, vzG91, CG14]). It states that if $\gcd(n, q-1) > 1$ and $q > n^4$ then there is no PP of degree n over $\mathbb{F}_q$.

In [Car62], the author showed existence of PBs of the form $x^{\frac{q-1}{3}+1} + ax \in \mathbb{F}_q[x]$ for sufficiently large q. Subsequent improvements of this result, which will be discussed in somewhat more detail in Section 5.3, led to significantly precise estimate of the number of PBs ([MZ09]) and in general PPs of the form $x^r f(x^{\frac{q-1}{d}})$ ([AGW09]). However, despite all these improvements, precise count of PBs seems extremely difficult to obtain. Hence, a reasonable goal is to obtain enumeration results for specific classes of PBs.[7]

Apart from having inherent theoretical appeal, PPs (not necessarily univariate) have been considered in several practical contexts, such as in cryptography ([Lid85, Pat96, CCZ98, LM84, MP14]), coding theory ([Din13]), combinatorial designs (e.g. Mutually Orthogonal Latin Squares ([Man42, JDM61, Eva92, Zie13]), Tuscan k-arrays ([CG02]), Costas arrays ([GM96]), [DY06]), sequences ([BEP96]), construction of high-girth graphs ([DLW07]), etc.

For example, PPs, due to their bijective property, are used in various symmetric-key encryption schemes (in fact, the S-Box transformation in the much widely used AES encryption scheme is a permutation, namely $f(x) = x^{-1}, f(0) = 0$ over $\mathbb{F}_{2^8}$, see [DR02] for more details); there it is required that the PPs have *provable*, favorable cryptographic properties. Analyzing and mathematically establishing such properties becomes easier in case of polynomials with fewer terms, e.g., for monomials and binomials. In particular, for permutations used in S-Boxes of block ciphers it is required that they do not have any *linear structure* ([Eve88]).

[7] There is another line of research which focuses on enumeration of PPs according to degree. For example, it is easy to see that there are no PPs of degree 0 and there are exactly $q(q-1)$ PPs of degree 1 (the set of all linear polynomials). However, the problem of counting PPs of arbitrary degree also seems to be very difficult. See [KP02, Das02, KP06] for results in this direction.

Based on a result of [CS11] it can be shown that PBs of the form $x^{\frac{2^n-1}{d}+1} + ax \in \mathbb{F}_{2^n}[x]$ do not have linear structure. Hence, these PBs are potential candidates for use in S-Boxes.

Motivated by their theoretical as well as practical significance, there is a spurt in research interest in PPs, especially in the past twenty years. Several classes of PPs have been discovered and their properties have been investigated. Account of this relatively recent development can be found in [MP13, Hou15b].

These considerations motivate us to consider PBs, and revisit the problems of their characterization, existence and enumeration. We obtain exact solutions for these problems for binomials of the form $x^{\frac{2^n-1}{2^t-1}+1} + ax$ over $\mathbb{F}_{2^n}$, under certain restrictions. These PBs are of the form $x(x^{\frac{q-1}{d}} + a)$ over $\mathbb{F}_q$, which are closely related to orthomorphism binomials (to be discussed shortly). On the other hand, they belong to the class of cyclotomic mapping binomials (to be described shortly), i.e., binomials of the form $x^r(x^{\frac{q-1}{d}s} + a)$.

Hence, to rephrase our contribution, we obtain characterization, existence and enumeration results for certain cyclotomic mapping PBs over $\mathbb{F}_{2^n}$. Our choice of even characteristic is motivated by possible applications in cryptography. On the other hand, our consideration of cyclotomic mapping binomials is not completely arbitrary. Indeed, as the next proposition (also observed in [Hou15c]) whose proof is postponed to Appendix D shows, permutation property of any arbitrary binomial is somewhat related to permutation property of a cyclotomic mapping binomial. This partly explains our motivation behind considering this particular class.

Proposition 5.1.1. *The binomial $f(x) = x^m + ax^n \in \mathbb{F}_q[x]$, with $m > n$, can be transformed modulo $(x^q - x)$, into a binomial of the form $x^r(x^{\frac{q-1}{d}} + a)$ for some $d \mid q-1$.*

We conclude this subsection by briefly recalling basic details of cyclotomic mapping polynomials and orthomorphism polynomials.

Cyclotomic mapping polynomial. Let γ be a primitive element of $\mathbb{F}_q$, and $q-1 = de$, where $d, e \in \mathbb{N}$. Let C_0 be the set of d-th powers of $\mathbb{F}_q$, i.e., $C_0 = \{\gamma^{dj} | j \in \{0, \ldots, e-1\}\}$. So, C_0 is a subgroup of order e and index d of the multiplicative group $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Elements of the *factor group* F_q^*/C_0 are the *cyclotomic cosets* given by

$$C_i = \gamma^i C_0, i \in \{0, \ldots d-1\}.$$

Note that the cyclotomic cosets $C_i, i \in \{0, \ldots, d-1\}$ partition $\mathbb{F}_q^*$. Given $a_0, \ldots, a_{d-1} \in \mathbb{F}_q$, the r-th order *cyclotomic mapping* $f^r_{a_0,\ldots,a_{d-1}}$ of index d is defined as

$$f^r_{a_0,\ldots,a_{d-1}}(\alpha) \triangleq \begin{cases} 0, & \text{if } \alpha = 0 \\ a_i \alpha^r, & \text{if } \alpha \in C_i, i \in \{0, \ldots, d-1\} \end{cases}$$

The polynomial $f^r_{a_0,\ldots,a_{d-1}}(x) \in \mathbb{F}_q[x]$ of degree at most $q-1$, representing [8] the mapping $f^r_{a_0,\ldots,a_{d-1}}$ (we use the same notation for the mapping as well as for the unique polynomial representing it) is an r-th order cyclotomic mapping polynomial (CMP) of index d. In particular, for $r = 1$, the polynomial is simply termed a cyclotomic mapping polynomial of index d.

It is clear that any mapping $f : \mathbb{F}_q \mapsto \mathbb{F}_q$, with $f(0) = 0$, is a cyclotomic mapping of index $q-1$. In fact, for $d_1 \mid d_2$, any cyclotomic mapping of index d_1 is also a cyclotomic mapping of index d_2. Cyclotomic mappings of index $1, 2, 3, \ldots$, are called *linear, quadratic, cubic, ...*, cyclotomic mappings respectively.

It can be seen from the definition that linear CMPs are of the form $f(x) = ax$ for fixed $a \in \mathbb{F}_q$. Next proposition (see [Eva92, NW05, Wan13]) shows that r-th order CMPs of index d are essentially the polynomials of the form $x^r f(x^{\frac{q-1}{d}})$. For the sake of completeness, we give its proof in Appendix D.

Proposition 5.1.2. *For integers $r > 0$, and $d \mid q-1$, r-th order CMPs of index d are the polynomials of the form $x^r f(x^{\frac{q-1}{d}})$. Moreover, if the mapping $f^r_{a_0,\ldots,a_{d-1}}$ is represented by the unique polynomial $x^r \sum_{i=0}^{d-1} b_i x^{\frac{i(q-1)}{d}}$, then we have the following relations*

(i) $a_j = \sum_{i=0}^{d-1} b_i \gamma^{\frac{ji(q-1)}{d}}, j \in \{0, \ldots, d-1\},$

(ii) $b_i = \frac{1}{d} \sum_{j=0}^{d-1} a_j \gamma^{\frac{-ji(q-1)}{d}}, i \in \{0, \ldots, d-1\},$

where γ is a primitive element of $\mathbb{F}_q$.

The following theorem from [LW91] is a fundamental tool for analyzing permutation properties of CMPs, i.e., polynomials of the form $x^r f(x^{\frac{q-1}{d}})$. The theorem was reproven at various other places (see e.g., [Wan07, Zie09]). We also reprove it in Appendix D. Our proof of the theorem is somewhat different, though

[8] As noted in the beginning, any mapping $f : \mathbb{F}_q \mapsto \mathbb{F}_q$ can be represented by a unique polynomial of degree at most $q-1$.

slightly more involved than the proofs found in the literature. Here, we note that the case $r = 1$ was proven earlier in [NR82]. In fact, for our purpose the case $r = 1$ is sufficient.

Theorem 5.1.1 ([LW91]). *Let d, r be positive integers and q be a prime power such that d divides $q-1$. Let γ be a primitive element in $\mathbb{F}_q$, and $f \in \mathbb{F}_q[x]$. Then $g(x) = x^r f(x^{\frac{q-1}{d}})$ is a PP of $\mathbb{F}_q$ if and only if the following conditions are satisfied.*

1. $\gcd(r, \frac{q-1}{d}) = 1$,
2. *for all* i, *with* $0 \leq i < d$, $f(\gamma^{i\frac{q-1}{d}}) \neq 0$,
3. *for all* j, *with* $0 \leq i < j < d$, $g(\gamma^i)^{\frac{q-1}{d}} \neq g(\gamma^j)^{\frac{q-1}{d}}$.

It is not known whether Theorem 5.1.1 is an explicit characterization of CMPs, i.e., PPs of the form $x^r f(x^{\frac{q-1}{d}})$; computation of necessary and sufficient conditions of Theorem 5.1.1 requires computation of a primitive root of $\mathbb{F}_q$, which is not known to have an efficient algorithm (see e.g. [MP13]).

Theorem 5.1.1 reduces permutation property of the polynomial $g(x) = x^r f(x^{\frac{q-1}{d}})$ over $\mathbb{F}_q$ into permutation property of a related polynomial $g(x)^{\frac{q-1}{d}}$ over a smaller subset, the set of d-th roots of unity, of $\mathbb{F}_q$. If the smaller subset is chosen to be the multiplicative group of a subfield $\mathbb{F}_{q'}$ of $\mathbb{F}_q$ then the original polynomial $x^r f(x^{\frac{q-1}{d}})$ reduces to a polynomial of the form $y^r f(y)$ over $\mathbb{F}_{q'}$. With careful choices the polynomial $y^r f(y)$ turns out to be a polynomial whose permutation properties over $\mathbb{F}_{q'}$ are well-known, or can be easily analyzed. This approach was taken in ([Zie13, WLHZ14]), where the reduced polynomials are low degree (degree ≤ 5) polynomials explicitly characterized by Dickson (see [LN97] or [Zie13]) or Dickson polynomials.

We use Theorem 5.1.1 in our proof of Theorem 5.2.1 from Theorem 5.2.2. In the proof of Theorem 5.2.1, our approach is somewhat similar to the one described above. However, in our case (described in Section 5.2.1) , the reduced polynomial is more involved.

Results on permutation properties of cyclotomic mapping binomials, which are relevant to our contribution, are discussed in Section 5.2.1. For further information on permutation properties of CMPs, see [LW91, Eva92, Eva94, NW05, Zie10, Wan13].

Orthomorphism polynomials. First, we recall definition of orthomorphism and complete mapping.

Definition 5.6. Let $\mathbb{G}$ be a finite abelian group, written additively. A mapping $h : \mathbb{G} \mapsto \mathbb{G}$ is an *orthomorphism* if both the mappings $x \mapsto h(x)$ and $x \mapsto h(x) - x$ are bijective for $x \in \mathbb{G}$, and it is called *complete mapping* if both $x \mapsto h(x)$ and $x \mapsto h(x) + x$ are bijective.

By taking $\mathbb{G}$ to be the additive group of a finite field $\mathbb{F}_q$, *orthomorphism polynomials* and *complete mapping polynomials* can be naturally defined for finite fields. A polynomial $h(x) \in \mathbb{F}_q[x]$ is an orthomorphism (complete mapping) polynomial if both $h(x)$ and $h(x) - x$ ($h(x) + x$ respectively) are PPs. Here, we note that for finite fields of even characteristic orthomorphisms and complete mappings are same.

Example 5.2. For a finite field $\mathbb{F}_q$, the set of linear maps given by the polynomials $f_a(x) = ax, a \in \mathbb{F}_q,\ a \neq 0,\ 1\ (a \neq 0, -1)$ forms a set of $q - 2$ orthomorphisms (complete mappings).

Next proposition, which follows directly from Definition 5.6, establishes connection between PBs of the form $x(x^{\frac{q-1}{d}} + a)$ over $\mathbb{F}_{2^n}$ and orthomorphisms.

Proposition 5.7. *$x(x^{\frac{q-1}{d}} + a)$ is a PB of $\mathbb{F}_{2^n}$ if and only if $x(a^{-1}x^{\frac{q-1}{d}} + 1)$ is an orthomorphism.*

In fact, it can be immediately seen that, in the above case, $a^{-1}x^{\frac{q-1}{d}+1}$ is also an orthomorphism of $\mathbb{F}_{2^n}$.

Study of complete mappings begun in [Man42] in connection with construction of *mutually orthogonal latin squares* (MOLS). MOLS are extremely important statistical designs that are used in statistical experiments. Subsequently, in [Pai47, Pai51, HP55], conditions were obtained under which a group admits complete mapping. Orthomorphisms, though very much related to complete mappings, were formally introduced in [JDM61], also in connection with construction of MOLS. In Appendix D, we illustrate how orthomorphisms can be used to construct MOLS.[9]For further details on complete mappings and orthomorphisms, especially over finite fields, see [NR82, NR81, Eva92, Eva87, Eva89, Eva94, NW05] .

[9]Apart from various combinatorial designs, such as MOLS, transversal designs, generalized Hadamard matrices, Room squares, orthomorphisms were also used in the construction of check digit systems [Sch96, SW10, Win14], and multi-permutations (useful in cryptography) [SV95], etc.

5.2 EXISTING RESULTS AND OUR CONTRIBUTION

We divide the discussion on our contribution and relevant existing results into two parts - characterization and enumeration.

5.2.1 CHARACTERIZATION

In our first result, we explicitly characterize certain class of cyclotomic mapping PBs over $\mathbb{F}_{2^n}$. In order to motivate our result, first, we discuss relevant existing explicit characterizations. Subsequently, we discuss our contributions which are stated as Theorem 5.2.1 and Theorem 5.2.2.

Although our focus lies in explicit characterization of PBs, given in Theorem 5.2.1, crux of the proof of Theorem 5.2.1 is explicit characterization of permutation trinomials of specific form, given in Theorem 5.2.2. Explicit characterization is even more difficult and rare for permutation trinomials (see [Hou15b, DQW+15]). We do not discuss the few existing explicit characterizations as those are not relevant to our case, and also because our primary motivation is explicit characterization of PBs. We hope that our result on trinomials, presented in Theorem 5.2.2, will be a valuable addition to the theory.

EXISTING EXPLICIT CHARACTERIZATIONS

Below we discuss existing explicit characterizations of cyclotomic mapping PBs, i.e., PBs of the form $x^r(x^{\frac{q-1}{d}s} + a) \in \mathbb{F}_q[x]$, q even. [10]

1. In [Wan02], the author characterized PBs of the form $x^r(x^{\frac{q-1}{d}s} + 1) \in \mathbb{F}_q[x]$ for $d \in \{3, 5\}$, and in [AW05], characterization for $d = 7$ was settled. For the case $d = 3$ in [Wan02], the author used Hermite-Dickson criteria (Theorem 5.2). For the cases $d \in \{5, 7\}$, Hermite-Dickson criteria along with various properties of Fibonacci and Lucas sequences were used.

[10] PBs of the form $x^r(x^{es} + a)$ were characterized in [AW06, Wan07, Zie09] for considerably general setting of parameters. However, it is not clear whether those characterizations are explicit.

2. In [Zie13], the author characterized PBs of the form $(i)\ x^{\frac{q^2-1}{q-1}+1}+ax$ over $\mathbb{F}_{q^2}$, $(ii)\ x^{\frac{q^3-1}{q-1}+1}+ax$ over $\mathbb{F}_{q^3}$, for all characteristic. He used a variant of Theorem 5.1.1 to reduce the polynomials (in both the cases) into a polynomial of low degree (degree ≤ 5) over $\mathbb{F}_q$. Then he used characterizations of such low degree polynomials from Dickson's table. These two characterizations generalize the results of [GC15, TZH14, WLHZ14] pertaining to PBs of this form.

   In [BZ15b], the authors reproved the above two cases using different techniques. Along with Theorem 5.1.1 (the version given in [NR82]), they essentially used criteria for solvability of bivariate equations over $\mathbb{F}_q$.

3. In another line of work, characterization of PBs of the form $x^r(x^{\frac{q^2-1}{q+1}s}+a)$ over $\mathbb{F}_{q^2}$ was considered. Unlike in the above cases, in this case, it is not possible to reduce the polynomial to a polynomial over $\mathbb{F}_q$ using Theorem 5.1.1 (due to the form of the exponent $\frac{q^2-1}{q+1}$).

   In [Zie13], the author characterized this class under the restriction that a is a $(q+1)$-th root of unity. This characterization generalizes a similar characterization for even characteristic obtained in [TZHL13].

   PBs of the form $x^{2(q-1)+1}+ax$ and $x^{3(q-1)+1}+ax \in \mathbb{F}_{q^2}$ have been characterized in [Hou15a] and [dHL15] respectively. These are specific subclasses of PBs of the form $x^r(x^{\frac{q^2-1}{q+1}s}+a) \in \mathbb{F}_{q^2}$. Hermite-Dickson criteria, along with additional techniques, was used in both the cases.

OUR CONTRIBUTION

Our first result is explicit characterization of PBs of the form $f(x) = x^{\frac{2^n-1}{2^t-1}+1}+ax$, $a \in \mathbb{F}^*_{2^{2t}}$, where $n = 2^s t$. More precisely, our result is the following.

Theorem 5.2.1. *Let s and t be positive integers, and $n = 2^s t$. Then the polynomial $f(x) = x^{\frac{2^n-1}{2^t-1}+1}+ax$, $a \in \mathbb{F}^*_{2^{2t}}$, is a PB of $\mathbb{F}_{2^n}$ if and only if (i) t is odd,(ii) $s \in \{1,2\}$, and (iii) $a \in \omega\mathbb{F}^*_{2^t} \cup \omega^2\mathbb{F}^*_{2^t}$, where $\omega \in \mathbb{F}_{2^2}$ is a root of the equation $\omega^2+\omega+1=0$.*

The condition $a \in \omega\mathbb{F}^*_{2^t} \cup \omega^2\mathbb{F}^*_{2^t}$ in Theorem 5.3.1, is equivalent to the condition $a^{2(2^t-1)}+a^{2^t-1}+1=0$, and the latter can be checked in time $poly(t)$. So, Theorem 5.3.1 is indeed an explicit characterization of PBs of the form $x^{\frac{2^n-1}{2^t-1}+1}+ax$, $a \in \mathbb{F}^*_{2^{2t}}$.

Theorem 5.2.1 immediately leads to the following enumeration result.

Corollary 5.2.1. *Let $n = 2^s t, s \in \{1, 2\}$, and t be odd, then the number of $a \in \mathbb{F}^*_{2^{2t}}$ such that $x^{\frac{2^n-1}{2^t-1}+1} + ax$ is a PB of $\mathbb{F}_{2^n}$ is $2(2^t - 1)$. For t even, there is no such PB.*

The case $s = 1$ of Theorem 5.2.1 was proven in our earlier work [SBÇ12]. The proof, given there, is more direct than the one obtained as part of Theorem 5.2.1 (which uses characterization of Dickson polynomials). So, we also include the proof separately in Section 5.3.1. In fact, this special case was already proven in [CK08] as part of a more general result. There, classification of this type of PBs was used in the context of cubic monomial bent functions of Maiorana-McFarland class. However, the method used there is rather complex, and is based on the results related to Walsh spectrum of quadratic boolean functions. We derive the same result here using a direct application of Theorem 5.1.1 along with some very elementary techniques. Our proof is rather short and simple. As stated in item (2)-(*i*) above, this result was fully generalized, i.e., extended to odd characteristic, in the later work [Zie13].

Further impetus for characterization, in Theorem 5.2.1, came from the recent work ([WLHZ14]), where PBs of the form $x^{\frac{2^{st}-1}{2^t-1}+1} + ax$ over $\mathbb{F}_{2^{st}}$ were considered. There, the authors obtained sufficient conditions (to be PB) for this class for the following combinations: (*i*) $s = 3$ and $\gcd(t, 9) = 3$ (see [TZH14] for the case $s = 3$ and $\gcd(t, 9) = 1$) (*ii*) $s = 4$ and $\gcd(t, 4) = 1$, (*iii*) $s = 6$ and $\gcd(t, 6) = 1$, (*iv*) $s = 10$ and $\gcd(t, 10) = 1$.[11] In particular, we observed that while there are $a \in \mathbb{F}_{2^{2t}}$ such that $x^{\frac{2^{4t}-1}{2^t-1}+1} + ax$ is a PB over $\mathbb{F}_{2^{4t}}$, there are no such $a \in \mathbb{F}_{2^{2t}}$ such that $x^{\frac{2^{8t}-1}{2^t-1}+1} + ax$ is a PB. This observation is generalized in Theorem 5.2.1.

In a simultaneous and independent work ([BZ15a]), the authors have characterized PBs of the form $x^{\frac{2^{4t}-1}{2^t-1}+1} + ax$ over $\mathbb{F}_{2^{4t}}$. They have shown that for $t(\geq 4)$ even, there does not exist any PB of this form, and for $t(\geq 3)$ odd, they have characterized all PBs of this form. So, there is overlap of this result with Theorem 5.2.1 for the case $s = 2, a \in \mathbb{F}_{2^{2t}}$. However, their approach, in this case, is similar to [BZ15b], and is different from ours.

[11] In [WLHZ15], the authors extended these results to odd characteristic for the cases $s \in \{4, 6\}$ under various restrictions.

Here, we highlight the fact that while we restrict a to the subfield $\mathbb{F}_{2^{2t}}$ of $\mathbb{F}_{2^n}$, the setting for $n(=2^s t)$ is considerably general than the previously discussed cases of [Zie13, WLHZ14, TZH14, BZ15b, BZ15a]; in all these cases, n is of the form 2^{st} for specific values of s only. Also, we note that Theorem 5.2.1 is essentially a non-existence result (apart from the cases $s = 1, 2$). However, it does not follow from the other well-known non-existence results such as Carlitz-Wan conjecture, not even for large enough n (with respect to t). It would be interesting to see if analogous non-existence results hold for odd characteristics as well.

Our approach (discussed in more detail in Section 5.3.2), in the proof of Theorem 5.2.1, is different from those of [Zie13, WLHZ14, BZ15b, BZ15a] to some extent. In our case, we use Theorem 5.1.1 to reduce (preserving permutation property) the the polynomial $x^{\frac{2^n-1}{2^t-1}+1} + ax \in \mathbb{F}_n[x]$, $n = 2^s t, a \in \mathbb{F}^*_{2^{2t}}$ to a trinomial of the form $x^{2^s+1} + x^{2^{s-1}+1} + \alpha x$ over $\mathbb{F}_{2^t}$. To (explicitly) characterize trinomials of the form $x^{2^s+1} + x^{2^{s-1}+1} + \alpha x$, where $s \geq 3$, we use Hermite-Dickson criteria (Theorem 5.2). For $0 \leq s \leq 2$, we use known characterization of low degree PPs from Dickson's table and characterization of Dickson polynomials. More formally, explicit characterization of trinomials of the form $x^{2^s+1} + x^{2^{s-1}+1} + \alpha x$ is the following.

Theorem 5.2.2. *$x^{2^s+1} + x^{2^{s-1}+1} + \alpha x \in \mathbb{F}_{2^t}[x]$, is a PP of $\mathbb{F}_{2^t}$ if and only if (i) t is odd,(ii) $\alpha = 1$, and (iii) $s \in \{1, 2\}$.*

Theorem 5.2.2 forms the crux of the proof of Theorem 5.2.1. Though our main motivation is to prove Theorem 5.2.1, as a result Theorem 5.2.2 may be of independent interest. More so, because permutation properties of trinomials are much less known.

5.2.2 ENUMERATION

Genesis of the line of work on enumeration of PBs can be traced batck to the work [Car62]. There, the author showed that, for sufficiently large q, there is $a \in \mathbb{F}_q$ such that $x^{\frac{q-1}{3}+1}+ax$ is a PB. Later, in [CW66], this result was extended for general d. In [WMS95], number of such PBs was estimated to be $\frac{d!}{d^d}q + O(\sqrt{q})$. This estimate was refined and extended in [LC07, MZ09]. In particular, in [MZ09], the following estimate was obtained.

Theorem 5.8. *Pick integers $0 < n < m$ such that $\gcd(m, n, q-1) = 1$, and suppose that $q \geq 4$. If $\gcd(m-n, q-1) > \frac{2q(\log\log q)}{\log q}$, then there exists $a \in \mathbb{F}_q^*$ such that $x^m + ax^n$ permutes $\mathbb{F}_q$. Further let T denote the number of $a \in \mathbb{F}_q$ for which $x^m + ax^n$ permutes $\mathbb{F}_q$, and putting $d := \frac{q-1}{\gcd(m-n,q-1)}$, we have*

$$\frac{q - 2\sqrt{q} + 1}{d^{d-1}} - (d-3)\sqrt{q} - 2 \leq \frac{T}{(d-1)!} \leq \frac{q + 2\sqrt{q} + 1}{d^{d-1}} + (d-3)\sqrt{q}$$

These results are general, in the sense that they are applicable for a wide class of binomials. Though they present an overall picture, their accuracy is limited when it comes to specific cases. So, it is naturally motivating to make the above results precise, at least in specific cases.

OUR CONTRIBUTION

In our next result, we partially enumerate PBs of the form $x(x^{\frac{2^n-1}{3}} + a) \in \mathbb{F}_{2^n}[x]$, where $n = 2^s t, a \in \mathbb{F}_{2^t}$. For the special case of $t = 1$, we only prove existence of these PBs. This can be thought of as a proof of Carlitz'z result ([Car62]), mentioned earlier, in even characteristic, using much elementary techniques and with more precision.

Theorem 5.2.3. *Let $n = 2^s t$, where $t \geq 1$ is odd and $s \geq 1$ is any integer. Then*

1. *for $t > 1$, the number of PBs of the form $x(x^{\frac{2^n-1}{3}} + a) \in \mathbb{F}_{2^n}[x]$, where $a \in \mathbb{F}_{2^t}$ is*

$$\begin{cases} \frac{2^{t+1}-7}{3}, \text{ when } t = 0 \bmod (3); \\ \frac{2^{t+1}-4}{3}, \text{otherwise}; \end{cases}$$

2. *for $t = 1$, there exists $a \in \mathbb{F}_{2^n}$ such that $x(x^{\frac{2^n-1}{3}} + a) \in \mathbb{F}_{2^n}[x]$ is a PB.*

Interestingly, for $t > 1$ case, our result indicates that the density of elements $a \in \mathbb{F}_{2^t}$ such that $x(x^{\frac{2^n-1}{3}} + a)$ is a PP is higher than the density of those elements in $\mathbb{F}_{2^n}$. In the former case, density given by Theorem 5.2.3 is $\approx \frac{2}{3}$, while in the latter case, density given by Theorem 5.8 is $\approx \frac{2}{9}$. This information is useful when such PBs are constructed by randomly sampling a from $\mathbb{F}_{2^n}$, which is a method of choice since there is no known efficient deterministic algorithm to construct a s. Our result shows that sampling from smaller subfield $\mathbb{F}_{2^t}$ is more likely to produce a PB of this form than sampling from the field $\mathbb{F}_{2^n}$.

5.3 Proofs

5.3.1 Explicit characterization of PBs of the form $x^{2^t+2} + ax$ over $\mathbb{F}_{2^{2t}}$

Theorem 5.3.1. *Let $t \geq 3$ and $a \in \mathbb{F}^*_{2^{2t}}$. Then for t odd, $x^{2^t+2} + ax \in \mathbb{F}_{2^{2t}}[x]$ is a PB iff $a^{2^t-1} \in \{\omega, \omega^2\}$, i.e., iff $a \in \omega\mathbb{F}^*_{2^t} \bigcup \omega^2\mathbb{F}^*_{2^t}$. For t even, there is no such PB of this form.*

Proof. First, we observe that for $f(x) = x^{2^t+2} + ax$ to be a PB it is necessary that $a \in \mathbb{F}^*_{2^{2t}} \setminus \mathbb{F}^*_{2^t}$; otherwise, $f(x) = 0$ has two distinct solutions in $\mathbb{F}_{2^t}$. Next, we note that $x^{2^t+2} + ax = x(x^{\frac{2^{2t}-1}{2^t-1}} + a)$. So, we check conditions of Theorem 5.1.1 to find if $f(x)$ is a PB. The first condition is trivially satisfied. Let γ be a primitive element of $\mathbb{F}_{2^{2t}}$. Then for $0 \leq i < 2^t - 1$, $\gamma^{(2^t+1)i} \in \mathbb{F}^*_{2^t}$. So, by the observation made at the beginning, it follows that the second condition is also satisfied.

Hence, $f(x)$ is a PB if and only if the last condition of Theorem 5.1.1 is satisfied, where we need to show that f^{2^t+1} is injective over the domain $\{\gamma^i : 0 \leq i < 2^t - 1\}$. First, we note that for $0 \leq i < 2^t - 1$, $(\gamma^{2^t+1})^i$ runs through all the elements of $\mathbb{F}^*_{2^t}$. Hence, it remains to show that $g : \mathbb{F}^*_{2^t} \mapsto \mathbb{F}^*_{2^t}$, defined as $g(\alpha) = \alpha(\alpha + a)^{2^t+1}$, is injective over $\mathbb{F}^*_{2^t}$. Now, for $\alpha \in \mathbb{F}^*_{2^t}$, $g(\alpha) = \alpha(\alpha+a)^{2^t+1} = \alpha^3+(a^{2^t}+a)\alpha^2+a^{2^t+1}\alpha$.[12] We simplify further by making the substitution $\alpha = \beta+a^{2^t}+a$ in $g(\alpha)$. Therefore, the final condition is that $f(x)$ is a PB if and only if the mapping h, defined as $h(\beta) = \beta^3 + (a^{2^{t+1}} + a^2 + a^{2^t+1})\beta$, is injective over the domain $\mathbb{F}_{2^t} \setminus \{a^{2^t} + a\}$. Next, we consider the following two cases.

Case 1. t odd: Here, we claim that h is injective iff $a^{2^{t+1}} + a^2 + a^{2^t+1} = 0$. For, if the condition holds then h, defined as $h(\beta) = \beta^3$, is injective because $\gcd(3, 2^t - 1) = 1$ for odd t. Next, if $a^{2^{t+1}} + a^2 + a^{2^t+1} \neq 0$ then $h(\beta) = 0$ for $\beta = 0$ and $\beta = a^{2^t} + a + a^{2^{2t-1}+2^{t-1}}$. Now, we have $(a^{2^t} + a + a^{2^{2t-1}+2^{t-1}})^2 = a^{2^{t+1}} + a^2 + a^{2^t+1} \neq 0$. So, $a^{2^t} + a + a^{2^{2t-1}+2^{t-1}} \neq 0$. Hence, h is not injective.

We note that $a^{2^{t+1}}+a^2+a^{2^t+1} = a^2((a^{2^t-1})^2+a^{2^t-1}+1)$. Therefore, $a^{2^{t+1}}+a^2+a^{2^t+1} = 0$ iff a^{2^t-1} is a root of the equation $x'^2 + x' + 1 = 0$ in $\mathbb{F}_{2^{2t}}$, i.e., $a^{2^t-1} \in \{\omega, \omega^2\}$, i.e., $a \in \omega\mathbb{F}^*_{2^t} \bigcup \omega^2\mathbb{F}^*_{2^t}$.

[12] Here, we note that $g(y) \in \mathbb{F}_{2^t}[y]$ as $(a^{2^t} + a)^{2^t} = a^{2^t} + a$ and $(a^{2^t+1})^{2^t-1} = 1$ are both in $\mathbb{F}_{2^t}$.

Case 2. t even: In this case, if $a^{2^{t+1}}+a^2+a^{2^t+1} \neq 0$ then by the previous argument it follows that h is not injective over the domain $\mathbb{F}_{2^t} \setminus \{a^{2^t}+a\}$. If $a^{2^{t+1}}+a^2+a^{2^t+1} = 0$ then h, defined as $h(\beta) = \beta^3$, is not injective, because for even t, $3 \mid 2^t - 1$. □

5.3.2 EXPLICIT CHARACTERIZATION OF PBS OF THE FORM $x^{\frac{2^{2^s t}-1}{2^t-1}+1} + ax, a \in \mathbb{F}^*_{2^{2t}}$

Theorem 5.2.1. *Let s and t be positive integers, and $n = 2^s t$. Then the polynomial $f(x) = x^{\frac{2^n-1}{2^t-1}+1} + ax$, $a \in \mathbb{F}^*_{2^{2t}}$, is a PB of $\mathbb{F}_{2^n}$ if and only if (i) t is odd,(ii) $s \in \{1,2\}$, and (iii) $a \in \omega\mathbb{F}^*_{2^t} \cup \omega^2\mathbb{F}^*_{2^t}$, where $\omega \in \mathbb{F}_{2^2}$ is a root of the equation $\omega^2 + \omega + 1 = 0$.*

Our proof of Theorem 5.2.1 is through explicit characterization of permutation trinomials of the form given in Theorem 5.2.2. More specifically, we have:

Theorem 5.2.2. *$x^{2^s+1} + x^{2^{s-1}+1} + \alpha x \in \mathbb{F}_{2^t}[x]$, is a PP of $\mathbb{F}_{2^t}$ if and only if (i) t is odd,(ii) $\alpha = 1$, and (iii) $s \in \{1,2\}$.*

In the next subsection, we state results that we will use in our proofs. In the subsequent subsection, first we prove Theorem 5.2.2, and then Theorem 5.2.1.

5.3.2.1 TOOLS

Hermite-Dickson criteria and Lucas' theorem (Theorem 5.9) are our main tools in our proof of Theorem 5.2.2; in fact, we use a corollary (Corollary 5.10) of Lucas' theorem. Finally, we derive Theorem 5.2.1 from Theorem 5.2.2 by applying Theorem 5.1.1. Next, we state Lucas' theorem.

Theorem 5.9 (Lucas (see [LN97])). *Let p be a prime, and $n, r_1, r_2, \ldots, r_t$ be non-negative integers such that*

$$n = d_0 + d_1 p + d_2 p^2 + \ldots + d_s p^s \ (0 \leq d_i \leq p-1, \forall\, 0 \leq i \leq s)$$
$$r_j = d_{j0} + d_{j1} p + d_{j2} p^2 + \ldots + d_{js} p^s \ (0 \leq d_{ji} \leq p-1, \forall\, 1 \leq j \leq t, \forall\, 0 \leq i \leq s)$$

Then

$$\binom{n}{r_1, r_2, \ldots, r_t} = \binom{d_0}{d_{10}, d_{20}, \ldots, d_{t0}} \cdots \binom{d_s}{d_{1s}, d_{2s}, \ldots, d_{ts}} \mod (p)$$

We will need the following corollary of the above theorem.

Corollary 5.10. $\binom{n}{r_1, r_2, \ldots, r_t} \neq 0 \mod (p)$ *iff* $\sum_{i=1}^{t} d_{ij} = d_j, \forall\, 0 \leq j \leq s$.

Let $a = \sum_{i=0}^{l} a_i 2^i$ be the 2-adic representation of a, then we denote by a_i the ith bit [13] of a. For example, $a = 2$ has base-2 representation 10; its 0th bit is 0, and 1st bit is 1. Also, let $\mathrm{wt}(a) \triangleq |\{i | a_i \neq 0\}|$.

5.3.2.2 PROOF OF THEOREM 5.2.2

Proof. First, we note that it is sufficient to consider the cases with $s < t$. For $s \geq t$, $f(x) = x^{2^s+1} + x^{2^{s-1}+1} + \alpha x$ can be reduced modulo $x^{2^t} + x$ to get a polynomial $x^{2^{s'}+1} + x^{2^{s'-1}+1} + \alpha x, s' < t$, which induces identical mapping on $\mathbb{F}_{2^t}$.

Next, we consider the cases corresponding to $s = 0, 1, 2$. For these cases we directly refer to the work of Dickson [Dic96] (see also [LN97]), where all PPs of degree ≤ 5 for all characteristics were characterized. The characterization is in terms of *reduced* or *normalized* polynomials. A polynomial $f(x)$ of degree n is normalized if *i*) $f(x)$ is monic *ii*) $f(0) = 0$, and *iii*) when degree of $f(x)$ is not divisible by the characteristic, coefficient of the term of degree $n - 1$ is zero.

For $s = 0$, we have $f(x) = x^2 + x^{2^{t-1}+1} + \alpha x$. Here, we note that $f(x)$ is a PP iff $g(x) = f(x)^2 \bmod (x^{2^t} + x)$ is a PP. Now, $g(x) = f(x)^2 \mod (x^{2^t} + x) = x^4 + x^3 + \alpha^2 x^2$. So, $g(x)$ is in normalized form and it follows from [Dic96] that $g(x)$ is not a PP of $\mathbb{F}_{2^t}$ for any t.

Similarly, it also follows from [Dic96] that for the cases $s = 1$ and $s = 2$, $f(x)$ is a PP of $\mathbb{F}_{2^t}$ iff t is odd and $\alpha = 1$. In fact, for $s = 2, \alpha = 1$, $f(x) = x^5 + x^3 + \alpha x$ is the *Dickson polynomial*, $D_5(x, 1)$, which is a PP of $\mathbb{F}_{2^t}$ iff $\gcd(2^{2t} - 1, 5) = 1$; this is true if and only if t is odd.

Now, we show that $f(x)$ is not a PP for $s \geq 3$ by applying the Hermite-Dickson criteria (Theorem 5.2). For this, we raise $f(x)$ to $2^t - 3$ and $2^t - 4$ modulo $(x^{2^t} + x)$, and show that the degree of the resulting polynomial is $2^t - 1$ in at least one of the two cases. Here, it is important to note that for any polynomial $g(x) \in \mathbb{F}_{2^t}[x]$, exactly those terms whose exponents are multiples of $2^t - 1$ reduce to the term with exponent $2^t - 1$ when $g(x)$ is reduced modulo $x^{2^t} + x$. More precisely, and specifically for our case, we state the following fact, which we will use later.

[13] We will use the abbreviation 'bit' for binary digit.

Fact 5.1. *Let* $g(x) = \sum_i a_i x^i \in \mathbb{F}_{2^t}[x]$, *and let* $g(x) \bmod (x^{2^t} + x) = b_{2^t-1}x^{2^t-1} + \sum_{i=0}^{2^t-2} b_i x^i$. *Then* $b_{2^t-1} = \sum_{j, 2^t-1|j} a_j$

Hence, we will be done if we can show that sum of the coefficients of the terms, whose exponents are multiples of $2^t - 1$ in the expansion of $f(x)^{2^t-3}$ or $f(x)^{2^t-4}$ modulo $(x^{2^t} + x)$, is non-zero. To show this, we first consider the expansion $f(x)^{2^t-3} \bmod (x^{2^t} + x)$ and then $f(x)^{2^t-4} \bmod (x^{2^t} + x)$. We show that if, in the first case, the sum is zero then it is non-zero in the second case. Though the approaches are similar in these two cases, they are not exactly same.

Case 1. $f(x)^{2^t-3} \bmod (x^{2^t} + x)$**:** First, we point out that coefficient of a term whose exponent is $\ell(2^t - 1), \ell \geq 1$, in the expansion of $f(x)^{2^t-3} \bmod (x^{2^t} + x)$ is $(\binom{2^t-3}{u,v,w} \bmod (2))\alpha^w$, where $0 \leq u, v, w \leq 2^t - 3$ are such that the following conditions hold

$$u + v + w = 2^t - 3, \tag{5.1}$$

$$(2^s + 1)u + (2^{s-1} + 1)v + w = \ell(2^t - 1). \tag{5.2}$$

Let $\mathcal{S} = \{(u, v, w, \ell) | u, v, w, \ell$ non-negative, and satisfies (5.1) and (5.2)$\}$. Our goal is to obtain the sum $\sum_{(u,v,w,\ell)\in\mathcal{S}} (\binom{2^t-3}{u,v,w} \bmod (2))\alpha^w$. To do this, we split the sum into parts according to the value of ℓ, and investigate contribution from each part.

Henceforth, for this case, whenever we write $\binom{2^t-3}{u,v,w}$, we implicitly assume values of u, v, w that satisfy, possibly along with some other constraints, (5.1) and (5.2) for some ℓ, whose value will be clear from the context. Also, we have the following observation.

Observation 5.1. 1*st bit of* $2^t - 3$ *is zero. Hence, if any of* $u, v, w \in \{2, 3\} \bmod (4)$ *then following Corollary 5.10* $\binom{2^t-3}{u,v,w} = 0 \bmod (2)$.

Next, (5.2)−(5.1) yields

$$2^s u + 2^{s-1} v = 2^t(\ell - 1) - (\ell - 3). \tag{5.3}$$

Clearly, both u and v can not be zero at the same time. Now, since $t > s$, we have from (5.3), $\ell = 3 \bmod (2^{s-1})$. Also, from (5.1) and (5.2), $\ell \leq 2^s + 1$. So, possible values of ℓ are 3 and $2^{s-1} + 3$. We consider the following two subcases based on these two values of ℓ.

– *Subcase 1.1.* $\ell = 3$: In this case, (5.3) yields $v = 2^{t-s+2} - 2u$. We consider the following subcases depending on $\mathrm{wt}(u)$.

– *Subsubcase 1.1.1.* $\mathrm{wt}(u) > 1$: Let the first $k (k \geq 1)$ consecutive bits of u be 1, i.e., $u = \sum_{j=i_1-k+1}^{i_1} 2^j + \sum_{j=0}^{i_2} u_j 2^j$, where $i_1 \leq t-s$, $i_2 \leq i_1 - k - 1$, $u_j \in \{0,1\}, 0 \leq j \leq i_2$, and if $k = 1$ then at least one u_j is non-zero (since $\mathrm{wt}(u) > 1$). So, $v = 2^{t-s+2} - \sum_{j=i_1-k+2}^{i_1+1} 2^j - \sum_{j=1}^{i_2+1} u_{j-1} 2^j$. Hence, $v = 2^{i_1+2} - \sum_{j=i_1-k+2}^{i_1+1} 2^j - \sum_{j=1}^{i_2+1} u_{j-1} 2^j \mod (2^{i_1+2})$, since $i_1 + 2 \leq t - s + 2$. Now, $2^{i_1+2} - \sum_{j=i_1-k+2}^{i_1+1} 2^j = 2^{i_1-k+2}$, and $\sum_{j=1}^{i_2+1} u_j 2^j < 2^{i_2+2} \leq 2^{i_1-k+1}$. So, $v \mod (2^{i_1+2}) \leq 2^{i_1-k+2}$, and $v \mod (2^{i_1+2}) > 2^{i_1-k+2} - 2^{i_1-k+1} = 2^{i_1-k+1}$. Now, we have the following two possibilities.

(i) $v \mod (2^{i_1+2}) < 2^{i_1-k+2}$: In this case, $(i_1 - k + 1)$-th bit of v is 1, since $v \mod (2^{i_1+2}) > 2^{i_1-k+1}$. So, $(i_1 - k + 1)$-th bits of both u and v are 1. Hence, following Corollary 5.10, $\binom{2^t-3}{u,v,w} = 0 \mod (2)$.

(ii) $v = 2^{i_1-k+2} \mod (2^{i_1+2})$: In this case, we note that $k > 1$. Since otherwise, at least one u_j in the sum $\sum_{j=0}^{i_2} u_j 2^j$, appearing in the binary representation of u, is non-zero. This implies $v < 2^{i_1-k+2} \mod (2^{i_1+2})$, a contradiction. Now, for $k > 1$, $(i_1 - k + 2)$-th bit of both u and v are 1. So, again $\binom{2^t-3}{u,v,w} = 0 \mod (2)$.

– *Subsubcase 1.1.2.* $\mathrm{wt}(u) \leq 1$: For $\ell = 3$, (5.3) implies $u \leq 2^{t-s+1}$. Also, if $u = 1$ then $v = 2^{t-s+2} - 2u$, i.e., $v = 2 \mod (4)$. So, by Observation 5.1, $\binom{2^t-3}{u,v,w} = 0 \mod (2)$. For the remaining possible values of u, i.e., for $u = 0$ or 2^i, with $2 \leq i \leq t - s + 1$, we examine the bit patterns of u, v, w in Table 5.1. For better understanding, we illustrate the case $t = 9, s = 3, i = 4$ in Table 5.2.

TABLE 5.1

Values		Bit positions with 1
$u = 0$, $v = 2^{t-s+2}$, $w = 2^t - 2^{t-s+2} - 3$	u	$\emptyset$
	v	$\{t - s + 2\}$
	w	$\{r \mid r = 0,$ $2 \leq r \leq t - s + 1,$ $t - s + 3 \leq r \leq t - 1\}$
$u = 2^i$, $v = 2^{t-s+2} - 2^{i+1}$, $w = 2^t - 2^{t-s+2} + 2^i - 3$ $(2 \leq i \leq t - s + 1)$	u	$\{i\}$
	v	$\{r \mid i + 1 \leq r \leq t - s + 1\}$
	w	$\{r \mid r = 0,$ $2 \leq r \leq i - 1,$ $t - s + 2 \leq r \leq k - 1\}$

TABLE 5.2

Value	Bit representation									
$2^t - 3 = 2^9 - 3$	1	1	1	1	1	1	1	1	0	1
$u = 2^4$	0	0	0	0	0	1	0	0	0	0
$v = 2^8 - 2^5$	0	0	1	1	1	0	0	0	0	0
$w = 2^9 - 2^8 + 2^4 - 3$	0	1	0	0	0	0	1	1	0	1

From Table 5.1, it can be observed that for these $t - s + 1$ values of u, none of u, v, w has 1 in the 1st bit position; each of u, v, w has 0 in the t-th bit position. For any other bit position r, where $0 \leq r \leq k-1$, $r \neq 1$, exactly one among u, v, w has 1 in the r-th position. Therefore, for each of these $t - s + 1$ values of u, $\binom{2^t-3}{u,v,w} = 1 \mod (2)$.

So, coefficient of the term with exponent $3(2^t - 1)$ in the expansion of $f(x)^{2^t-3} \bmod (x^{2^t} + x)$ is $\alpha^{2^t-2^{t-s+2}-3}(1 + \sum_{i=2}^{t-s+1} \alpha^{2^i})$.

– *Subcase 1.2.* $\ell = 2^{s-1} + 3$: For $\ell = 2^{s-1}+3$, (5.3) yields $v = 2^{t-s+2}(2^{s-2}+1)-2u-1$. When $u = 0 \mod (4)$, $v = 3 \mod (4)$, since $s \geq 3$ and $t > s$. So, v has 1 in the 1st bit position. Hence, by Observation 5.1 $\binom{2^t-3}{u,v,w} = 0 \mod (2)$. Next, From (5.1) and (5.2), we get $w = u - 2^{t-s+2} - 2$. Hence, for $u = 1 \mod (4)$, $w = 3 \mod (4)$, which, by Observation 5.1, implies $\binom{2^t-3}{u,v,w} = 0 \mod (2)$. Again using Observation 5.1, $\binom{2^t-3}{u,v,w} = 0 \mod (2)$ for $u = 2$, or $3 \mod (4)$.

Hence, considering the above cases, we get that the coefficient of the term with exponent $2^t - 1$ in the expansion of $f(x)^{2^t-3} \bmod (x^{2^t} + x)$ is $\alpha^{2^t-2^{t-s+2}-3}(1 + \sum_{i=2}^{t-s+1} \alpha^{2^i})$. Therefore, if $1 + \sum_{i=2}^{t-s+1} \alpha^{2^i} \neq 0$ then $x^{2^s+1} + x^{2^{s-1}+1} + x$, with $3 \leq s < t$, is not a PP of $\mathbb{F}_{2^t}$. Otherwise, i.e., if

$$\sum_{i=2}^{t-s+1} \alpha^{2^i} = 1, \tag{5.4}$$

we consider the next case.

Case 2. $f(x)^{2^t-4} \bmod (x^{2^t}+x)$**:** Similar to equations (5.1), (5.2), and (5.3) from the previous case, we get from the expansion of $f(x)^{2^t-4} \bmod (x^{2^t}+x)$ the following set of equations (in this case, $0 \leq u, v, w \leq 2^t - 4$, and $\ell \geq 0$).

$$u + v + w \;=\; 2^t - 4 \tag{5.5}$$

$$(2^s+1)u+(2^{s-1}+1)v+w = \ell(2^t-1) \quad (5.6)$$

$$2^s u+2^{s-1}v = 2^t(\ell-1)-(\ell-4) \quad (5.7)$$

As in the previous case, when we write $\binom{2^t-4}{u,v,w}$, we mean values of u, v, w that satisfy (5.5), (5.6) (and thereby (5.7)) for some ℓ, which is clear from the context. Here, we have the following observation.

Observation 5.2. *0-th bit and 1st bit of* 2^t-4 *are zero. So, if any of* $u, v, w \in \{1,2,3\} \mod (4)$ *then following Corollary 5.10* $\binom{2^t-4}{u,v,w} = 0 \mod (2)$.

Next, following similar considerations as in Case 1, from (5.7), we get for this case $\ell \in \{4, 2^{s-1}+4\}$. Now, for $\ell = 2^{s-1}+4$, $v = 2^{t-s+1}(2^{s-1}+3)-2u-1$. Since, $t > s$, $v \in \{1,3\} \mod (4)$. This implies, by Observation 5.2, $\binom{2^t-4}{u,v,w} = 0 \mod (2)$. So, we are left with the $\ell = 4$ case. Next, we consider the following subcases of $\ell = 4$ case.

– *Subcase 2.1.* $\mathrm{wt}(u) \leq 1$: In this case, $u = 0$, or $u = 2^i$, with $0 \leq i \leq t-s+1$ (upper bound on i follows from (5.7)). Now, if $i \in \{0,1\}$ then following Observation 5.2, $\binom{2^t-4}{u,v,w} = 0 \mod (2)$. Also, for $i = t-s+1$, $v = 2^{t-s+1}$. So, both u and v have 1 in $(t-s+1)$-th bit position. This again implies $\binom{2^t-4}{u,v,w} = 0 \mod (2)$ for $i = t-s+1$. For the remaining values of i, we show the bit patterns of u, v, w in Table 5.3. In Table 5.4, we illustrate the case for $t = 11, s = 4, i = 5$. From Table 5.3 it is clear that $\binom{2^t-4}{u,v,w} = 1 \mod (2)$ for these $t-s$ values of u.

TABLE 5.3

Values		Bit positions with 1
$u = 0$, $v = 2^{t-s+2}+2^{t-s+1}$, $w = 2^t-2^{t-s+2}-2^{t-s+1}-4$	u	$\emptyset$
	v	$\{t-s+2, t-s+1\}$
	w	$\{r \mid 2 \leq r \leq t-s,$ $t-s+3 \leq r \leq t-1\}$
$u = 2^i$, $v = 2^{t-s+2}+2^{t-s+1}-2^{i+1}$, $w = 2^t-2^{t-s+2}-2^{t-s+1}+2^i-4$ $(2 \leq i \leq t-s)$	u	$\{i\}$
	v	$\{r \mid r = t-s+2,$ $i+1 \leq r \leq t-s\}$
	w	$\{r \mid 2 \leq r \leq i-1,$ $r = t-s+1,$ $t-s+3 \leq r \leq k-1\}$

TABLE 5.4

Value	Bit representation											
$2^t - 4 = 2^{11} - 4$	1	1	1	1	1	1	1	1	1	1	0	0
$u = 2^5$	0	0	0	0	0	0	1	0	0	0	0	0
$v = 2^9 + 2^8 - 2^6$	0	0	1	0	1	1	0	0	0	0	0	0
$w = 2^{10} + 2^8 + 2^5 - 4$	0	1	0	1	0	0	0	1	1	1	0	0

– *Subcase 2.2.* $\mathrm{wt}(u) > 1$: Let the first $k(k \geq 1)$ consecutive bits of u be 1, i.e., $u = \sum_{j=i_1-k+1}^{i_1} 2^j + \sum_{j=0}^{i_2} u_j 2^j$, where $i_1 \leq t - s + 1, i_2 \leq i_1 - k - 1, u_j \in \{0, 1\}, 0 \leq j \leq i_2$, and if $k = 1$ then at least one u_j is non-zero. Next, we consider the following subcases.

– *Subsubcase 2.2.1.* $i_1 \leq t - s$: We note that $v = 2^{t-s+2} + 2^{t-s+1} - 2u$, i.e., $v = 2^{t-s+1} + (2^{t-s+2} - 2u)$. Now, from the analysis of the Subsubcase 1.1.1 ($\mathsf{wt(u) > 1}$) of Case 1, we have that both u and $2^{t-s+2} - 2u$ have 1 in the r-th bit position, where $r \leq i_1 \leq t - s$. Then it is easy to see that both u and $2^{t-s+2} + 2^{t-s+1} - 2u$ has 1 in the same r-th bit position. So, following Corollary 5.10, $\binom{2^t-4}{u,v,w} = 0 \mod (2)$ in this case.

– *Subsubcase 2.2.2.* $i_1 = t - s + 1$: We have the following two possibilities.

(i) $\mathrm{wt}(u - 2^{t-s+1}) \geq 2$: So, $v = 2^{t-s+2} + 2^{t-s+1} - 2u = 2^{t-s+1} - 2u'$, where $u' = u - 2^{t-s+1}$, and $\mathrm{wt}(u') \geq 2$. Let $u' = 2^j + \sum_{m=0}^{j-1} u_m 2^m$, $u_m \in \{0, 1\}$, and at least one $u_m = 1$. It is clear that $j \leq t - s - 1$; otherwise, $v < 0$. But this is equivalent to the Subsubcase 1.1.1 ($\mathsf{wt(u) > 1}$) of Case 1, which implies u' and v has 1 in the same rth bit position for some $r \leq t - s - 1$. This, in turn, implies u and v has 1 in the same (as the previous) r-th bit position. Hence, we get that $\binom{2^t-4}{u,v,w} = 0 \mod (2)$ in this case as well.

(ii) $\mathrm{wt}(u - 2^{t-s+1}) = 1$: Let us assume that $u = 2^{t-s+1} + 2^j$, where $2 \leq j \leq t - s$. In Table 5.5, we consider bit patterns of u, v, w for this case. Bit patterns from Table 5.5 imply that for these $t - s - 1$ values of j, $\binom{2^t-4}{u,v,w} = 1 \mod (2)$.

TABLE 5.5

Values	Bit positions with 1	
$u = 2^{t-s+1} + 2^j$, $v = 2^{t-s+1} - 2^{j+1}$, $w = 2^t - 2^{t-s+2} + 2^j - 4$ $(2 \leq j \leq t - s)$	u	$\{j, t - s + 1\}$
	v	$\{r \mid j + 1 \leq r \leq t - s\}$
	w	$\{r \mid 2 \leq r \leq j - 1,$ $t - s + 2 \leq r \leq t - 1\}$

So, considering the above possibilities, we conclude that the coefficient of the term with exponent $4(2^t-1)$, in the expansion of $f(x)^{2^t-4} \bmod (x^{2^t}+x)$, is

$$\alpha^{2^t-2^{t-s+2}-2^{t-s+1}-4}(1+\sum_{i=2}^{t-s}\alpha^{2^i})+\alpha^{2^t-2^{t-s+2}-4}\sum_{i=2}^{t-s}\alpha^{2^i}. \tag{5.8}$$

Now, by employing (5.4) and simplifying, we get that (5.8) equals $\alpha^{2^t-2^{t-s+2}+2^{t-s+1}-4}$, which is non-zero. From earlier discussion, coefficient of the term with exponent $(2^{s-1}+4)(2^t-1)$, in the expansion of $f(x)^{2^t-4} \bmod (x^{2^t}+x)$, is 0. So, the coefficient of the term with exponent 2^t-1, in the expansion of $f(x)^{2^t-4} \bmod x^{2^t}+x$, is clearly non-zero. □

5.3.2.3 Proof of Theorem 5.2.1

Proof. We apply Theorem 5.1.1 by setting $g(x)=x(x^{\frac{2^n-1}{2^t-1}}+a)$. Since $r=1$ in this case, condition (i) of Theorem 5.1.1 is satisfied. Next, we observe that condition (ii) of Theorem 5.1.1 is satisfied if and only if $a \in \mathbb{F}^*_{2^{2t}} \setminus \mathbb{F}^*_{2^t}$. So, $g(x)$ is a PP if and only if condition (iii) of Theorem 5.1.1 is satisfied for $a \in \mathbb{F}^*_{2^{2t}} \setminus \mathbb{F}^*_{2^t}$.

Let γ be a primitive element of $\mathbb{F}_{2^n}$. Then $\beta=\gamma^{\frac{2^n-1}{2^t-1}}$ is a primitive element of $\mathbb{F}_{2^t}$. So, for all $0 \le i < j < 2^t-1$, $g(\gamma^i)^{\frac{2^n-1}{2^t-1}} \neq g(\gamma^j)^{\frac{2^n-1}{2^t-1}}$ is equivalent to the condition

$$\beta^i(\beta^i+a)^{\frac{2^n-1}{2^t-1}} \neq \beta^j(\beta^j+a)^{\frac{2^n-1}{2^t-1}}, \text{ for } a \in \mathbb{F}^*_{2^{2t}} \setminus \mathbb{F}^*_{2^t} \text{ and } i \neq j.$$

For $a \in \mathbb{F}^*_{2^{2t}} \setminus \mathbb{F}^*_{2^t}$, the above condition implies $x(x+a)^{\frac{2^n-1}{2^t-1}}$ is a PP of $\mathbb{F}_{2^t}$. Hence, $g(x)$ is a PP of $\mathbb{F}_{2^n}$ if and only if $x(x+a)^{\frac{2^n-1}{2^t-1}}$ is a PP of $\mathbb{F}_{2^t}$ for $a \in \mathbb{F}^*_{2^{2t}} \setminus \mathbb{F}^*_{2^t}$. Let $\mathbb{F}_{2^{2t}}=\mathbb{F}_{2^t}(\zeta)$, where ζ is a root of the irreducible polynomial $x^2+x+\theta \in \mathbb{F}_{2^t}[x]$. So, we have

$$\zeta+\zeta^{2^t}=1 \tag{5.9}$$

Hence, $a \in \mathbb{F}^*_{2^{2t}} \setminus \mathbb{F}^*_{2^t}$ can be written as $a=b+c\zeta$, where $b,c \in \mathbb{F}_{2^t}, c \neq 0$. So,

$$\begin{aligned} x(x+a)^{\frac{2^n-1}{2^t-1}} &= x(x+b+c\zeta)^{\frac{2^{2^s t}-1}{2^t-1}} \\ &= x(x+b+c\zeta)^{2^{(2^s-1)t}+2^{(2^s-2)t}+\cdots+1} \\ &= x(x+b+c\zeta)^{2^{(2^s-1)t}}(x+b+c\zeta)^{2^{(2^s-2)t}}\ldots(x+b+c\zeta) \end{aligned}$$

$$= x\prod_{i=1}^{2^{s-1}}(x+b+c\zeta^{2^t})(x+b+c\zeta)$$

(By noting that for odd ℓ, $(x+b+c\zeta)^{2^{\ell t}} = (x+b+c\zeta^{2^t})$, and for even ℓ, $(x+b+c\zeta)^{2^{\ell t}} = (x+b+c\zeta)$.)

$$= x\prod_{i=1}^{2^{s-1}}(x^2+cx+b^2+bc+c^2\zeta+c^2\zeta^2)$$

(Using Equation 5.9, and after some regular calculations.)

$$= c^{2^s}\left(x^{2^s+1}+x^{2^{s-1}+1}+\left(\frac{b^2+bc+c^2\zeta+c^2\zeta^2}{c^2}\right)^{2^{s-1}}x\right)$$

(By the transformation $x \mapsto cx$.)

Since $b, c,$ and $\zeta^2+\zeta = \theta \in \mathbb{F}_{2^t}^*$, we have $\frac{b^2+bc+c^2\zeta+c^2\zeta^2}{c^2} \in \mathbb{F}_{2^t}^*$. Next, by applying Theorem 5.2.2 on the polynomial $x^{2^s+1}+x^{2^{s-1}+1}+\left(\frac{b^2+bc+c^2\zeta+c^2\zeta^2}{c^2}\right)^{2^{s-1}}x$, we get that $x(x+a)^{\frac{2^n-1}{2^t-1}}$ is a PP of $\mathbb{F}_{2^t}$ if and only if (i) t is odd,(ii) $s = 1, 2$, and (iii) $\frac{b^2+bc+c^2\zeta+c^2\zeta^2}{c^2} = 1$, i.e., $b^2+bc+c^2(1+\zeta+\zeta^2) = 0$.

Now, we have

$$\begin{aligned} a^{2^{t+1}}+a^2+a^{2^t+1} &= (b+c\zeta)^{2^{t+1}}+(b+c\zeta)^2+(b+c\zeta)^{2^t+1} \\ &= ((b+c\zeta)^{2^t})^2+(b+c\zeta)^2+(b+c\zeta)(b+c\zeta)^{2^t} \\ &= (b+c(1+\zeta))^2+(b+c\zeta)^2+(b+c\zeta)(b+c(1+\zeta)) \end{aligned}$$

(By employing Equation 5.9.)

$$= b^2+bc+c^2(1+\zeta+\zeta^2)$$

So, condition (iii) above is equivalent to $a^{2^{t+1}}+a^2+a^{2^t+1} = 0$.

Finally, as in the proof of Theorem 5.3.1, we make the above condition succinct by noting that $a^{2^{t+1}}+a^2+a^{2^t+1} = a^2((a^{2^t-1})^2+a^{2^t-1}+1)$. Therefore, $a^{2^{t+1}}+a^2+a^{2^t+1} = 0$ if and only if a^{2^t-1} is a root of the equation $x'^2+x'+1 = 0$ in $\mathbb{F}_{2^{2t}}$, i.e., $a^{2^t-1} \in \{\omega, \omega^2\}$, i.e., $a \in \omega\mathbb{F}_{2^t}^* \bigcup \omega^2\mathbb{F}_{2^t}^*$.

□

5.3.3 EXISTENCE AND ENUMERATION RESULTS OF PERMUTATION BINOMIALS OF THE FORM $x^{\frac{2^n-1}{3}+1} + ax \in \mathbb{F}_{2^n}[x]$

Theorem 5.2.3. *Let $n = 2^s t$, where $t \geq 1$ is odd and $s \geq 1$ is any integer. Then*

1. *for $t > 1$, the number of PBs of the form $x(x^{\frac{2^n-1}{3}} + a) \in \mathbb{F}_{2^n}[x]$, where $a \in \mathbb{F}_{2^t}$ is*

$$\begin{cases} \frac{2^{t+1}-7}{3}, \text{ when } t = 0 \bmod (3); \\ \frac{2^{t+1}-4}{3}, \text{otherwise;} \end{cases}$$

2. *for $t = 1$, there exists $a \in \mathbb{F}_{2^n}$ such that $x(x^{\frac{2^n-1}{3}} + a) \in \mathbb{F}_{2^n}[x]$ is a PB.*

5.3.3.1 TOOLS

Main tool in our proof of Theorem 5.2.3 is Theorem 5.1.1 and some properties of the *Norm* map. More formally, given an extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$, the Norm map $N_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \mapsto \mathbb{F}_q$ is defined as $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \triangleq \alpha^{\frac{q^m-1}{q-1}}$. We will use the following known properties (see [LN97] for details) of the Norm map.

1. For $\alpha, \beta \in \mathbb{F}_{q^m}$, $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha\beta) = N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)$.
2. For $\beta \in \mathbb{F}_q^*$, $|\{\alpha \in \mathbb{F}_{q^m}^* | N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \beta\}| = \frac{q^m-1}{q-1}$.
3. For $r|m$, $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(N_{\mathbb{F}_{q^m}/\mathbb{F}_{q^r}}(\alpha))$.
4. For $\alpha \in \mathbb{F}_q$, $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha^m$; this essentially follows from property 1.

5.3.3.2 PROOF OF THEOREM 5.2.3

Proof. Let γ be a primitive element of $\mathbb{F}_{2^n}$ and $\omega = \gamma^{\frac{2^n-1}{3}}$. So, ω is a primitive cube root of unity, i.e., $\mathbb{F}_{2^2}^* = \{1, \omega, \omega^2\}$. Hence, by Theorem 5.1.1, $x(x^{\frac{2^n-1}{3}} + a), a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^2}$, is a PB of $\mathbb{F}_{2^n}$ if and only if

$$(1+a)^{\frac{2^n-1}{3}}, \omega(\omega+a)^{\frac{2^n-1}{3}}, \omega^2(\omega^2+a)^{\frac{2^n-1}{3}}$$

, are all distinct, i.e.,

***Condition* 5.1.**

$$N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(1+a), \omega N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(\omega+a), \omega^2 N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(\omega^2+a)$$

are all distinct.

Now, we consider the two cases separately.

Case 1. $t > 1$**:** First, we settle the following claims.

***Claim* 5.1.** *For* $\alpha \in \mathbb{F}_{2^t}^*$, $N_{\mathbb{F}_{2^{2t}}/F_{2^2}}(\alpha) = 1$.

Proof. For $\alpha \in \mathbb{F}_{2^t}^*$, $N_{\mathbb{F}_{2^{2t}}/F_{2^2}}(\alpha) = \alpha^{\frac{2^{2t}-1}{3}} = \alpha^{\frac{(2^t-1)(2^t+1)}{3}} = 1$, since for odd t, $3 \mid (2^t+1)$. □

***Claim* 5.2.** *For* $\alpha \in \mathbb{F}_{2^t}^*, \beta \in \mathbb{F}_{2^2}^*$, *if* $N_{\mathbb{F}_{2^n}/F_{2^2}}(\alpha+\omega) = \beta$, *then* $N_{\mathbb{F}_{2^n}/F_{2^2}}(\alpha+\omega^2) = \beta^2$.

Proof. For $\beta \in \mathbb{F}_{2^2}$ and t odd, we have

$$\begin{aligned}
\beta^2 = \beta^{2^t} &= (N_{\mathbb{F}_{2^n}/\,\mathbb{F}_{2^2}}(\alpha+\omega))^{2^t} \\
&= N_{\mathbb{F}_{2^n}/\,\mathbb{F}_{2^2}}((\alpha+\omega)^{2^t}) \text{ (follows from property 1 of Norm map)} \\
&= N_{\mathbb{F}_{2^n}/\,\mathbb{F}_{2^2}}((\alpha+\omega^{2^t})) \\
&= N_{\mathbb{F}_{2^n}/\,\mathbb{F}_{2^2}}((\alpha+\omega^2))
\end{aligned}$$

□

Next, we note that cosets of $\mathbb{F}_{2^t}$ in $\mathbb{F}_{2^{2t}}$ can be written as $\mathbb{F}_{2^t} + \alpha\omega$, where $\alpha \in \mathbb{F}_{2^t}^*$. Our next claim is that the Norm $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(.)$ maps equal number of elements from every coset of $\mathbb{F}_{2^t}$ in $\mathbb{F}_{2^{2t}}$ to a fixed element in $\mathbb{F}_{2^2}$.

***Claim* 5.3.** $\forall \alpha \in \mathbb{F}_{2^t}^*, \beta \in \mathbb{F}_{2^2}^*, |\{\zeta \in \mathbb{F}_{2^t} | N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\zeta+\alpha\omega) = \beta\}| = |\{\zeta \in \mathbb{F}_{2^t} | N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\zeta+\omega) = \beta\}|$.

Proof. For $\zeta \in \mathbb{F}_{2^t}$ we have

$$\begin{aligned}
N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\zeta+\alpha\omega) &= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\alpha(\alpha^{-1}\zeta+\omega)) \\
&= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\alpha) N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}((\alpha^{-1}\zeta+\omega)) \\
&= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}((\alpha^{-1}\zeta+\omega)), \text{ since } N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\alpha) = 1 \text{ for } \alpha \in \mathbb{F}_{2^t}^*
\end{aligned}$$

So, the claim follows by the bijectivity of the mapping $\zeta \mapsto \alpha^{-1}\zeta$ for $\alpha \in \mathbb{F}_{2^t}^*$. □

Fact 5.2.

$$N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(\omega) = \begin{cases} 1 & \text{if } t = 0 \bmod (3), \\ \omega & \text{if } t = 1 \bmod (3) \text{ and } s \text{ is odd, or } t = 2 \bmod (3) \text{ and } s \text{ is even}, \\ \omega^2 & \text{if } t = 1 \bmod (3) \text{ and } s \text{ is even, or } t = 2 \bmod (3) \text{ and } s \text{ is odd}; \end{cases}$$

and similarly

$$N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(\omega^2) = \begin{cases} 1 & \text{if } t = 0 \bmod (3), \\ \omega^2 & \text{if } t = 1 \bmod (3) \text{ and } s \text{ is odd, or } t = 2 \bmod (3) \text{ and } s \text{ is even}, \\ \omega & \text{if } t = 1 \bmod (3) \text{ and } s \text{ is even, or } t = 2 \bmod (3) \text{ and } s \text{ is odd}. \end{cases}$$

Proof. Following property 4 of Norm, we have $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(\omega) = \omega^{2^{s-1}t}$, also (by property 1) $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(\omega^2) = (N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(\omega))^2$. The result follows from these two observations. □

For $a \in \mathbb{F}_{2^t} \setminus \{\mathbb{F}_{2^2}\}$, $a+1 \in \mathbb{F}^*_{2^t}$. Hence, from Claim D.1 and property 3 of Norm it follows that $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(1+a) = N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{2t}}}(1+a)) = N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}((1+a)^{2^{s-1}}) = (N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(1+a))^{2^{s-1}} = 1$. Also, following Claim 5.2, $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega^2) = 1$ when $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega) = 1$, and $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega^2) = \omega^2$ when $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega) = \omega$. Hence, Condition 5.1 is satisfied only in the cases when (*i*) $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega) = 1$, or (*ii*) $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega) = \omega$. But cardinality of the set $\{a \in \mathbb{F}_{2^t} \setminus \mathbb{F}_{2^2} \mid N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega) = 1 \text{ or } \omega\}$ is given by $2^t - 2 - |\{a \in \mathbb{F}_{2^t} \setminus \mathbb{F}_{2^2} \mid N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega) = \omega^2\}$. So, it is sufficient to find cardinality of the set $\{a \in \mathbb{F}_{2^t} \setminus \mathbb{F}_{2^2} \mid N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega) = \omega^2\}$.

From property 2 of Norm and Claim 5.3 it follows that

$$\begin{aligned} |\{a \in \mathbb{F}_{2^t} | N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a+\omega) = \omega\}| &= |\{a \in \mathbb{F}_{2^t} \mid N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a+\omega) = \omega^2\}| \\ &= \frac{1}{2^t-1}\frac{2^{2t}-1}{3} \\ &= \frac{2^t+1}{3}. \end{aligned}$$

Further, by the previous argument, $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega) = (N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a+\omega))^{2^{s-1}}$. Hence, $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega) = N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a+\omega)$ if s is odd, and $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega) = N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a+\omega^2)$ if s is even. So, for both the cases we have $|\{a \in \mathbb{F}_{2^t} \mid N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega) = \omega\}| = \frac{2^t+1}{3}$.

However, following Fact 5.2, either $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(0+\omega) = \omega^2$ or $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(1+\omega) = \omega^2$ (but not both) when $t \neq 0 \bmod (3)$. Hence, we have

$$|\{a \in \mathbb{F}_{2^t} \setminus \mathbb{F}_{2^2} \mid N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega) = \omega^2\}| = \begin{cases} \frac{2^t+1}{3}, & \text{when} t = 0 \bmod (3) \\ \frac{2^t-2}{3}, & \text{otherwise.} \end{cases}$$

Therefore, the result follows.

Case 2. $t = 1$**:** Here, we consider the following two subcases.

– *Subcase 2.1.* $s = 3$*:* In this case, we have $n = 8$ and the field is $\mathbb{F}_{2^8}$. By direct computation it can be shown that there exists an $a \in \mathbb{F}_{2^8} \setminus \mathbb{F}_{2^2}$ such that $N_{\mathbb{F}_{2^8}/\mathbb{F}_{2^2}}(1+a) = N_{\mathbb{F}_{2^8}/\mathbb{F}_{2^2}}(\omega+a) = N_{\mathbb{F}_{2^8}/\mathbb{F}_{2^2}}(\omega^2+a) = 1$. Therefore, we have

$$\{(1+a)^{\frac{2^n-1}{3}}, \omega(\omega+a)^{\frac{2^n-1}{3}}, \omega^2(\omega^2+a)^{\frac{2^n-1}{3}}\} = \{1, \omega, \omega^2\}.$$

– *Subcase 2.2.* $s \geq 4$*:* First, we note that if $\alpha \in \mathbb{F}_{2^8}$ then

$$N_{\mathbb{F}_{2^s}/\mathbb{F}_{2^2}}(\alpha) = N_{\mathbb{F}_{2^8}/\mathbb{F}_{2^2}}(N_{\mathbb{F}_{2^s}/\mathbb{F}_{2^8}}(\alpha)) = N_{\mathbb{F}_{2^8}/\mathbb{F}_{2^2}}(\alpha^{2^{s-3}}) = (N_{\mathbb{F}_{2^8}/\mathbb{F}_{2^2}}(\alpha))^{2^{s-3}}.$$

This implies that for a obtained in the previous subcase, we have

$$N_{\mathbb{F}_{2^s}/\mathbb{F}_{2^2}}(1+a) = N_{\mathbb{F}_{2^s}/\mathbb{F}_{2^2}}(\omega+a) = N_{\mathbb{F}_{2^s}/\mathbb{F}_{2^2}}(\omega^2+a) = 1.$$

Consequently,

$$\{(1+a)^{\frac{2^n-1}{3}}, \omega(\omega+a)^{\frac{2^n-1}{3}}, \omega^2(\omega^2+a)^{\frac{2^n-1}{3}}\} = \{1, \omega, \omega^2\}.$$

Hence, the result follows. □

Remark 5.11.

1. There is an error in [SBÇ12] in the expression obtained for Case 1 ($t > 1$), which we have corrected here.
2. For Case 2, a (whose existence has been proven) essentially belongs to $\mathbb{F}_{2^8}$. For this $a \in \mathbb{F}_{2^8}$, we obtain a PB $x(x^{\frac{2^n-1}{3}} + a) \in \mathbb{F}_{2^n}[x]$ for all $n = 2^s, s \geq 3$.

5.4 CONCLUSION

In this part of the thesis, motivated by their theoretical as well as practical significance, we have considered PBs over finite fields of even characteristic. There are very few classes or PBs for which explicit characterization is known. First, we have formalized the idea of explicit characterization in terms of computational complexity of evaluating corresponding necessary and sufficient conditions. Then we have explicitly characterized permutation binomials of the form $x^{\frac{2^{2^s t}-1}{2^t-1}+1} + ax$, $a \in \mathbb{F}^*_{2^{2t}}$. These extends very recent results of [WLHZ14, BZ15b, BZ15a] in various directions. It would be interesting to explore permutation properties of this class of binomials by removing the restriction $a \in \mathbb{F}^*_{2^{2t}}$, and also for analogous setting in odd characteristic.

Our second result is on the existence and enumeration of the class of permutation binomials of the form $x^{\frac{2^n-1}{3}+1} + ax \in \mathbb{F}_{2^n}[x]$. Our result is, in fact, Carlitz's result [Car62] for even characteristic, although using only elementary techniques (Carlitz's proof uses heavy machinery from algebraic geometry) and with more precision, in the sense that for all n, which are not powers of 2, we have given exact number of $a \in \mathbb{F}_{2^t}$ such that $x^{\frac{2^n-1}{3}+1} + ax$ is a PB of $\mathbb{F}_{2^n}$. Like in the previous case, it would be interesting to remove the restriction $a \in \mathbb{F}_{2^t}$. Also, from practical point of view it is worth studying relevant cryptographic properties of these permutation binomials with regard to their use in S-boxes of block ciphers.

Appendix D

Deferred Details

Proofs

Proposition 5.1.1. *The binomial $f(x) = x^m + ax^n \in \mathbb{F}_q[x]$, with $m > n$, can be transformed modulo $(x^q - x)$, into a binomial of the form $x^r(x^{\frac{q-1}{d}} + a)$ for some $d \mid q-1$.*

Proof. We have $f(x) = x^n(x^{m-n} + a)$. Let $\gcd(m-n, q-1) = e$. Then, there are $s, t \in \mathbb{Z}$ such that $s(m-n) + t(q-1) = e$. So, $s(\frac{m-n}{e}) + t(\frac{q-1}{e}) = 1$, and we have $\gcd(s, (\frac{q-1}{e})) = 1$. Let $\ell \in \mathbb{Z}$ be such that $\ell = s \mod (\frac{q-1}{e})$, and $\gcd(\ell, e) = 1$. Indeed, the following argument shows that such an integer exists.

Since $\gcd(s, (\frac{q-1}{e})) = 1$, it follows from Dirichlet's theorem (see [Apo76]) that there are infinitely many primes of the form $s + u(\frac{q-1}{e}), u \in \mathbb{N}$. However, e has only finitely many prime divisors. So, there is a prime $p \nmid e$ of the form $s+u(\frac{q-1}{e})$, with $u \in \mathbb{N}$, for which $\gcd(p, e) = 1$.

Therefore, we have $\gcd(\ell, q-1) = 1$. Hence, $y \mapsto y^\ell$ is a bijection of $\mathbb{F}_q$. Now, by applying this transformation we have $f(y^\ell) = y^{n\ell}(y^{\ell(m-n)} + a) = y^{n\ell}(y^e + a) \mod (y^q - y)$. The polynomial in the last expression is of the form $x^r(x^{\frac{q-1}{d}} + a)$ for $de = q-1$. □

Remark D.1. Proof of Proposition 5.1.1 does not provide any efficient deterministic algorithm [1] for transforming any arbitrary binomial $f(x) = x^m + ax^n \in \mathbb{F}_q[x]$, with $m > n$, into a binomial of the form $x^r(x^{\frac{q-1}{d}} + a)$. However, it certainly indicates that permutation properties of binomials are *information theoretically* related to the permutation properties of binomials of the form $x^r(x^{\frac{q-1}{d}} + a)$.

Proposition 5.1.2. *For integers $r > 0$, and $d \mid q-1$, r-th order CMPs of index d are the polynomials of the form $x^r f(x^{\frac{q-1}{d}})$. Moreover, if the mapping $f^r_{a_0,\ldots,a_{d-1}}$ is represented by the unique polynomial $x^r \sum_{i=0}^{d-1} b_i x^{\frac{i(q-1)}{d}}$, then we have the following relations*

(i) $a_j = \sum_{i=0}^{d-1} b_i \gamma^{\frac{ji(q-1)}{d}}, j \in \{0, \ldots, d-1\}$,

(ii) $b_i = \frac{1}{d} \sum_{j=0}^{d-1} a_j \gamma^{\frac{-ji(q-1)}{d}}, i \in \{0, \ldots, d-1\}$,

where γ is a primitive element of $\mathbb{F}_q$.

Proof. First, we settle the following claim.

***Claim* D.1.** *Let $q-1 = de$, where $d, e \in \mathbb{N}$. A mapping $f : \mathbb{F}_q \mapsto \mathbb{F}_q$ is r-th order cyclotomic mapping of index d if and only if $f(\alpha x) = \alpha^r f(x)$ for all $x \in \mathbb{F}_q$ and for all $\alpha \in \mathbb{F}_q$ such that $\alpha^e = 1$.*

Proof. One direction (only if) is clear from the definition. For the other direction, let C_j be a coset of C_0, and $\beta, \zeta \in C_j$. Then clearly $\beta = \alpha\zeta$ for some $\alpha \in C_0$, i.e., for some α such that $\alpha^e = 1$. Then we have $\frac{f(\beta)}{\beta^r} = \frac{f(\alpha\zeta)}{(\alpha\zeta)^r} = \frac{\alpha^r f(\zeta)}{(\alpha\zeta)^r} = \frac{f(\zeta)}{\zeta^r}$. This implies f is cyclotomic mapping of order r and index d. □

Next, let $f^r_{a_0,\ldots,a_{d-1}}(x) = \sum c_i x^i \in \mathbb{F}_q[x]$. Hence, by Claim D.1, it follows that $\alpha^r f^r_{a_0,\ldots,a_{d-1}}(x) = \sum c_i \alpha^i x^i$ for all $x \in \mathbb{F}_q$, and for all $\alpha \in C_0$. This is true if and only if $\alpha^{i-r} = 1$ for all $\alpha \in C_0$, and for all i such that $c_i \neq 0$. This is possible if and only if $e \mid i-r$, i.e., $i = r + \ell(\frac{q-1}{d})$ for some $\ell \in \mathbb{N}$. Hence, the first part is proven.

Now, an element $\alpha \in C_j$ can be written as $\alpha = \gamma^{j+id}$ for some $0 \leq i < \frac{q-1}{d}$. So, from definition $a_j \alpha^r = \alpha^r \sum_{i=0}^{d-1} b_i \gamma^{\frac{ji(q-1)}{d}}$. Hence, (i) follows.

[1] Here, the notion of efficient algorithm is same as discussed before, i.e., an algorithm that runs in time $O(poly(\log q))$.

In order to show (*ii*), we note that the coefficient matrix for the set of equations

$$a_j = \sum_{i=0}^{d-1} b_i \gamma^{\frac{ji(q-1)}{d}}, j \in \{0, \ldots, d-1\}$$

is the Vandermonde matrix $V = (\gamma^{\frac{ji(q-1)}{d}})$. This matrix is non-singular, and its inverse is given by $V^{-1} = \frac{1}{d}(\gamma^{\frac{-ji(q-1)}{d}})$. □

Theorem 5.1.1 ([LW91]). *Let d, r be positive integers and q be a prime power such that d divides $q-1$. Let γ be a primitive element in $\mathbb{F}_q$, and $f \in \mathbb{F}_q[x]$. Then $g(x) = x^r f(x^{\frac{q-1}{d}})$ is a PP of $\mathbb{F}_q$ if and only if the following conditions are satisfied.*

1. $\gcd(r, \frac{q-1}{d}) = 1$,
2. *for all* i, *with* $0 \le i < d$, $f(\gamma^{i\frac{q-1}{d}}) \neq 0$,
3. *for all* j, *with* $0 \le i < j < d$, $g(\gamma^i)^{\frac{q-1}{d}} \neq g(\gamma^j)^{\frac{q-1}{d}}$.

Proof. Let $g(x) = x^r f(x^{\frac{q-1}{d}})$ be a PP. Then $\gcd(r, \frac{q-1}{d}) = 1$; otherwise, there are two elements $\alpha_1 \neq \alpha_2 \in \mathbb{F}_q$ of order d such that $g(\alpha_1) = g(\alpha_2)$. We also note that $f(\gamma^{i\frac{q-1}{d}}) \neq 0$ for $0 \le i < d$; otherwise, $g(\alpha) = 0$ for two distinct values of α. So, assuming conditions (1) and (2), we need to show that condition (3) holds if and only if $g(x)$ is a PP. Now, according to condition (1), $\gcd(r, \frac{q-1}{d}) = 1$. Hence, there are $s, t \in \mathbb{Z}$ such that

$$sr + t\frac{q-1}{d} = 1. \tag{D.1}$$

We first prove the *if* part and then *only-if* part.

(*If*) Let conditions (1) and (2) above hold. We show that if $g(x) = x^r f(x^{\frac{q-1}{d}})$ is not a PP then condition (3) does not hold. Let $0 \le i < j \le q-2$ be such that $\gamma^{ir} f(\gamma^{\frac{i(q-1)}{d}}) = \gamma^{jr} f(\gamma^{\frac{j(q-1)}{d}})$. Also, let $i_1 = i \mod (d)$, and $j_1 = j \mod (d)$. Then we claim that $i_1 \neq j_1$; otherwise, $f(\gamma^{\frac{i(q-1)}{d}}) = f(\gamma^{\frac{j(q-1)}{d}}) \neq 0$ (last inequality follows from condition (2)). Hence, we have

$$\begin{aligned}
&\gamma^{(i-j)r} = 1 \\
\Rightarrow &\gamma^{(i-j)sr} = 1 \\
\Rightarrow &\gamma^{(i-j)(1-t\frac{q-1}{d})} = 1 \\
\Rightarrow &\gamma^{i-j} = 1 \text{ since } d \mid i-j.
\end{aligned}$$

The last condition is impossible since γ is a primitive element, and $0 \leq i < j \leq q-2$. Now, from $\gamma^{ir} f(\gamma^{\frac{i(q-1)}{d}}) = \gamma^{jr} f(\gamma^{\frac{j(q-1)}{d}})$ we have $(\gamma^{ir} f(\gamma^{\frac{i(q-1)}{d}}))^{\frac{q-1}{d}} = (\gamma^{jr} f(\gamma^{\frac{j(q-1)}{d}}))^{\frac{q-1}{d}}$. But, then we have $(\gamma^{i_1 r} f(\gamma^{\frac{i_1(q-1)}{d}}))^{\frac{q-1}{d}} = (\gamma^{j_1 r} f(\gamma^{\frac{j_1(q-1)}{d}}))^{\frac{q-1}{d}}$ for $0 \leq i_1 < j_1 < d$. This contradicts condition (3).

(*Only if*) Here, we show that if condition (3) does not hold then $g(x)$ is not a PP. Let i, j, with $0 \leq i < j < d$, be such that $(\gamma^{ir} f(\gamma^{\frac{i(q-1)}{d}}))^{\frac{q-1}{d}} = (\gamma^{jr} f(\gamma^{\frac{j(q-1)}{d}}))^{\frac{q-1}{d}}$. Let $\zeta = \gamma^{\frac{q-1}{d}}$. So, ζ is a primitive d-th root of unity. So, we have

$$(\gamma^{ir} f(\zeta^i))^{\frac{q-1}{d}} = \zeta^{jr} (f(\zeta^j))^{\frac{q-1}{d}}$$

$$\Rightarrow \zeta^{jr} = \left(\frac{\gamma^{ir} f(\zeta^i)}{f(\zeta^j)} \right)^{\frac{q-1}{d}}$$

$$\Rightarrow \zeta^{j(1-t\frac{q-1}{d})} = \left(\frac{\gamma^{irs} f(\zeta^i)^s}{f(\zeta^j)^s} \right)^{\frac{q-1}{d}}$$

(raising both sides to s and substituting D.1 in l. h. s.)

$$\Rightarrow \zeta^j = \left(\frac{\gamma^{irs} f(\zeta^i)^s \zeta^{tj}}{f(\zeta^j)^s} \right)^{\frac{q-1}{d}}.$$

Let $\eta = \left(\frac{\gamma^{irs} f(\zeta^i)^s \zeta^{jt}}{f(\zeta^j)^s} \right)$. Then it follows that $\eta \neq \gamma^i$; otherwise, we have $\zeta^i = \zeta^j$, where $0 \leq i < j < d$. But, this is not possible since ζ is a primitive d-th root of unity. Next, we substitute the value of η and do some regular calculation to have the following relation.

$$\eta^r f(\eta^{\frac{q-1}{d}}) = \eta^r f(\zeta^j) = \gamma^{ir} f(\gamma^{\frac{i(q-1)}{d}}). \tag{D.2}$$

(D.2) shows that $g(x)$ is not a PP. □

Remark D.2. Theorem 5.1.1 was proven earlier in various other works [LW91, Wan07, Zie08, Zie09]. Main technique in those proofs is counting. In our proof of the theorem, we have shown explicit pair of distinct elements as "witnesses" of non-injectivity of $g(x)^{\frac{q-1}{d}}$ (in the *if* part) and $g(x)$ (in the *only if* part).

ORTHOMORPHISMS AND LATIN SQUARES

A *latin square* L of order n over an alphabet S of size n is an $n \times n$ array with entries from S, such that each element of S appears exactly once in each row and each column of L. An immediate example of a latin square of order n (for any n) is

Cayley table of any group of order n. Latin squares L_1 and L_2 of same order are said to be orthogonal if each ordered pair of elements of S occurs exactly once among the pairs $(L_1(i,j), L_2(i,j))$, where $1 \leq i, j \leq n$. Let $h : \mathbb{G} \mapsto \mathbb{G}$ be a mapping, where $\mathbb{G}$ is a finite abelian group of order n. We observe that $L(x,y) = h(x) + y$ is a latin square if and only if h is a permutation. We further observe that two latin squares L_1, L_2 given by the entries $L_1(x,y) = h_1(x) + y$ and $L_2(x,y) = h_2(x) + y$, where $h_1, h_2 : \mathbb{G} \mapsto \mathbb{G}$, are mutually orthogonal if and only if $h_1(x) - h_2(x)$ is a permutation. In [Zie13], the author used this method to construct *complete sets*[2] of MOLS of order q^2 and q^3 for different values of q. As an example, Theorem 5.3.1 shows that $x^{2^t+2} + ax$ over $\mathbb{F}_{2^{2t}}$ is a PB if and only if $a \in \omega\mathbb{F}^*_{2^t} \cup \omega^2\mathbb{F}^*_{2^t}$. Now, it follows that for such a fixed PB, the set of $2^{2t}-1$ PBs, given by $\{bx^{2^t+2}+acx | b, c \in \mathbb{F}_{2^t}$, with both not zero at the same time$\}$, corresponds to a complete set of MOLS.

[2] A set of $n-1$ MOLS (maximum possible) of order n is termed complete.

Bibliography II

[AGW09] Amir Akbary, Dragos Ghioca, and Qiang Wang. On permutation polynomials of prescribed shape. *Finite Fields and Their Applications*, 15(2):195 – 206, 2009.

[AW05] Amir Akbary and Qiang Wang. On some permutation polynomials over finite fields. *International Journal of Mathematics and Mathematical Sciences*, 2005(16):2631–2640, 2005.

[AW06] Amir Akbary and Qiang Wang. A generalized lucas sequence and permutation binomials. *Proceedings of the American Mathematical Society*, 134(1):15–22, 2006.

[Apo76] Tom M Apostol. *Introduction to analytic number theory*, volume 1. Springer Science & Business Media, 1976.

[BZ15a] L.A. Bassalygo and V.A. Zinoviev. On one class of permutation polynomials over finite fields of characteristic two. In *The Ninth International Workshop on Coding and Cryptography (WCC) 2015*, 2015.

[BZ15b] L.A. Bassalygo and V.A. Zinoviev. Permutation and complete permutation polynomials. *Finite Fields and Their Applications*, 33(0):198 – 211, 2015.

[Bet51] Enrico Betti. Sopra la risolubilita per radicali delle equazioni algebriche irriduttibili di grado primo. *Ann. Sci. Mat. Fis.*, 2:49–115, 1851.

[Bet55] Enrico Betti. Sopra la teorica delle sostituzioni. *Ann. Sci. Mat. Fis.*, 6:5–34, 1855.

[BEP96] Simon R Blackburn, Tuvi Etzion, and Kenneth G Paterson. Permutation polynomials, de bruijn sequences, and linear complexity. *journal of combinatorial theory, Series A*, 76(1):55–82, 1996.

[Bri79] F Brioschi. Un teorema sulla teoria delle sostituzioni. *Rend. Reale Ist. Lombardo Sci. Lett.(2)*, 12:483–485, 1879.

[Bri70] Franc Brioschi. Des substitutions de la forme pour un nombren premier de lettres. *Mathematische Annalen*, 2(3):467–470, 1870.

[CCZ98] Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, bent functions and permutations suitable for des-like cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.

[Car62] L. Carlitz. Some theorems on permutation polynomials. *Bulletin of the American Mathematical Society*, 68(2):120–122, 03 1962.

[CW66] L. Carlitz and Charles Wells. The number of solutions of a special system of equations in a finite field. *Acta Arithmetica*, 12(1):77–84, 1966.

[CG14] Jasbir S. Chahal and Sudhir R. Ghorpade. Carlitz–wan conjecture for permutation polynomials and weil bound for curves over finite fields. *Finite Fields and Their Applications*, 28(0):282 – 291, 2014.

[CK08] Pascale Charpin and Gohar M. Kyureghyan. Cubic monomial bent functions: A subclass of $\mathcal{M}$. *SIAM Journal on Discrete Mathematics*, 22(2):650–665, 2008.

[CS11] Pascale Charpin and Sumanta Sarkar. Polynomials with linear structure and maiorana-mcfarland construction. *IEEE Transactions on Information Theory*, 57(6):3796–3804, 2011.

[CG02] Wensong Chu and Solomon W. Golomb. Circular tuscan-k arrays from permutation binomials. *Journal of Combinatorial Theory, Series A*, 97(1):195 – 202, 2002.

[CF95] S.D. Cohen and M.D. Fried. Lenstras proof of the carlitz-wan conjecture on exceptional polynomials: An elementary version. *Finite Fields and Their Applications*, 1(3):372 – 375, 1995.

[DR02] Joan Daemen and Vincent Rijmen. *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, 2002.

[Das02] Pinaki Das. The number of permutation polynomials of a given degree over a finite field. *Finite Fields and Their Applications*, 8(4):478 – 490, 2002.

[Dic96] Leonard Eugene Dickson. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *Annals of Mathematics*, 11(1/6):pp. 65–120, 1896.

[Dic58] Leonard Eugene Dickson. *Linear groups with an Exposition of the Galois Field Theory*. Dover, New York, 1958.

[Din13] Cunsheng Ding. Cyclic codes from some monomials and trinomials. *SIAM J. Discrete Math.*, 27(4):1977–1994, 2013.

[DQW+15] Cunsheng Ding, Longjiang Qu, Qiang Wang, Jin Yuan, and Pingzhi Yuan. Permutation trinomials over finite fields with even characteristic. *SIAM J. Discrete Math.*, 29(1):79–92, 2015.

[DY06] Cunsheng Ding and Jin Yuan. A family of skew hadamard difference sets. *Journal of Combinatorial Theory, Series A*, 113(7):1526 – 1535, 2006.

[DLW07] Vasyl Dmytrenko, Felix Lazebnik, and Jason Williford. On monomial graphs of girth eight. *Finite Fields and Their Applications*, 13(4):828–842, 2007.

[dHL15] Xiang dong Hou and Stephen D. Lappano. Determination of a type of permutation binomials over finite fields. *Journal of Number Theory*, 147(0):14 – 23, 2015.

[Eva87] Anthony B. Evans. Orthomorphisms of z_p. *Discrete mathematics*, 64(2):147–156, 1987.

[Eva89] Anthony B. Evans. Orthomorphisms of groups. *Annals of the New York Academy of Sciences*, 555(1):187–191, 1989.

[Eva92] Anthony B. Evans. *Orthomorphism graphs of groups*, volume 1535 of *Lecture Notes in Mathematics*. Springer, Berlin, 1992.

[Eva94] Anthony B. Evans. Cyclotomy and orthomorphisms. *Congressus Numerantium*, pages 97–108, 1994.

[Eve88] Jan-Hendrik Evertse. Linear structures in blockciphers. In David Chaum and WynL. Price, editors, *Advances in Cryptology — EUROCRYPT*, volume 304 of *Lecture Notes in Computer Science*, pages 249–266. Springer Berlin Heidelberg, 1988.

[GM96] Solomon W. Golomb and Oscar Moreno. On periodicity properties of costas arrays and a conjecture on permutation polynomials. *Information Theory, IEEE Transactions on*, 42(6):2252–2253, 1996.

[Gra81] A Grandi. Un teorema sulla rappresentazione analitica delle sostituzioni sopra un primo di elementi. *Giorn. Mat. Battaglini*, 19:238–245, 1881.

[Gra83] A Grandi. Generalizzazione di un teorema sulla rappresentazione analitica delle sostituzioni. *Rend. Reale Ist. Lombardo Sci. Lett.(2)*,

16:101–111, 1883.

[GC15] Xu Guangkui and Xiwang Cao. Complete permutation polynomials over finite fields of odd characteristic. *Finite Fields and Their Applications*, 31(0):228 – 240, 2015.

[HP55] Marshall Hall and L. J. Paige. Complete mappings of finite groups. *Pacific J. Math.*, 5(4):541–549, 1955.

[Her63] C. Hermite. Sur les fonctions de sept lettres. *C. R. Acad. Sci.*, 57(3):750–757, 1863.

[Hou15a] Xiang-dong Hou. Determination of a type of permutation trinomials over finite fields, {II}. *Finite Fields and Their Applications*, 35(0):16 – 35, 2015.

[Hou15b] Xiang-dong Hou. Permutation polynomials over finite fields a survey of recent advances. *Finite Fields and Their Applications*, 32:82–119, 2015.

[Hou15c] Xiang-dong Hou. A survey of permutation binomials and trinomials over finite fields. In *Topics in Finite Fields, Proceedings of the 11th International Conference on Finite Fields and Their Applications*, volume 632, pages 177–191. AMS, 2015.

[JDM61] Diane M Johnson, AL Dulmage, and NS Mendelsohn. Orthomorphisms of groups and orthogonal latin squares. *Canad. J. Math*, 13:356–372, 1961.

[Kay05] Neeraj Kayal. Recognizing permutation functions in polynomial time. *Electronic Colloquium on Computational Complexity (ECCC)*, (008), 2005.

[KP02] Sergei Konyagin and Francesco Pappalardi. Enumerating permutation polynomials over finite fields by degree. *Finite Fields and Their Applications*, 8(4):548 – 553, 2002.

[KP06] Sergei Konyagin and Francesco Pappalardi. Enumerating permutation polynomials over finite fields by degree ii. *Finite Fields and Their Applications*, 12(1):26–37, 2006.

[LC07] Yann Laigle-Chapuy. Permutation polynomials and applications to coding theory. *Finite Fields and Their Applications*, 13(1):58 – 70, 2007.

[LN73] Hans Lausch and Wilfried Nöbauer. *Algebra of polynomials*, volume 5. North-Holland Amsterdam, 1973.

[Lid85] R. Lidl. On cryptosystems based on polynomials and finite fields.

In Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, editors, *Advances in Cryptology*, volume 209 of *Lecture Notes in Computer Science*, pages 10–15. Springer Berlin Heidelberg, 1985.

[LM84] Rudolf Lidl and WinfriedB. Műller. Permutation polynomials in rsa-cryptosystems. In David Chaum, editor, *Advances in Cryptology*, pages 293–301. Springer US, 1984.

[LM88] Rudolf Lidl and Gary L. Mullen. When does a polynomial over a finite field permute the elements of the field? *The American Mathematical Monthly*, 95(3):pp. 243–246, 1988.

[LM93] Rudolf Lidl and Gary L. Mullen. When does a polynomial over a finite field permute the elements of the field?, ii. *The American Mathematical Monthly*, 100(1):pp. 71–74, 1993.

[LMT93] Rudolf Lidl, Gary Lee Mullen, and Gerhard Turnwald. *Dickson polynomials*, volume 65 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*. Longman Scientific & Technical, Harlow, 1993.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20. Cambridge University Press, 1997.

[LW91] Rudolf Lidl and Daqing Wan. Permutation polynomials of the form $x^r f(x^{\frac{q-1}{d}})$ and their group structure. *Monatshefte für Mathematik*, 112:149–164, 1991.

[LZ67] David London and Zvi Ziegler. Functions over the residue field modulo a prime. *Journal of the Australian Mathematical Society*, 7(03):410–416, 1967.

[MvzG94] Keju Ma and Joachim von zur Gathen. The computational complexity of recognizing permutation functions. In *Proceedings of the Twenty-sixth Annual ACM Symposium on Theory of Computing*, STOC '94, pages 392–401, New York, NY, USA, 1994. ACM.

[MVZG95a] Keju Ma and Joachim Von Zur Gathen. The computational complexity of recognizing permutation functions. *computational complexity*, 5(1):76–97, 1995.

[MVZG95b] Keju Ma and Joachim Von Zur Gathen. Tests for permutation functions. *Finite Fields and their applications*, 1(1):31–56, 1995.

[Man42] Henry B. Mann. The construction of orthogonal latin squares. *Ann. Math. Statist.*, 13(4):418–423, 12 1942.

[MZ09] Ariane Masuda and Michael Zieve. Permutation binomials over

finite fields. *Transactions of the American Mathematical Society*, 361(8):4169–4180, 2009.

[Mat61] Émile Mathieu. Mémoire sur l'étude des fonctions de plusieurs quantités, sur la maniere de les former et sur les substitutions qui les laissent invariables. *J. Math. Pures Appl*, 6:241–323, 1861.

[MP13] Gary L Mullen and Daniel Panario. *Handbook of finite fields*. CRC Press, 2013.

[MP14] Amela Muratovic-Ribic and Enes Pasalic. A note on complete polynomials over finite fields and their applications in cryptography. *Finite Fields and Their Applications*, 25:306–315, 2014.

[Nar84] Wladyslaw Narkiewicz. *Uniform distribution of sequences of integers in residue classes*. Springer, 1984.

[NR81] Harald Niederreiter and Karl H Robinson. Bol loops of order pq. *Mathematical Proceedings of the Cambridge Philosophical Society*, 89(2):241–256, 1981.

[NR82] Harald Niederreiter and Karl H Robinson. Complete mappings of finite fields. *Journal of the Australian Mathematical Society (Series A)*, 33(02):197–212, 1982.

[NW05] Harald Niederreiter and Arne Winterhof. Cyclotomic $\mathcal{R}$-orthomorphisms of finite fields. *Discrete mathematics*, 295(1):161–171, 2005.

[Nöb65] Wilfried Nöbauer. Über permutationspolynome und permutationsfunktionen für primzahlpotenzen. *Monatshefte für Mathematik*, 69(3):230–238, 1965.

[Pai47] L. J. Paige. A note on finite abelian groups. *Bull. Amer. Math. Soc.*, 53(6):590–593, 06 1947.

[Pai51] L. J. Paige. Complete mappings of finite groups. *Pacific J. Math.*, 1(1):111–116, 1951.

[Pat96] Jacques Patarin. Hidden fields equations (hfe) and isomorphisms of polynomials (ip): Two new families of asymmetric algorithms. In Ueli Maurer, editor, *Advances in Cryptology — EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Springer Berlin Heidelberg, 1996.

[SBÇ12] Sumanta Sarkar, Srimanta Bhattacharya, and Ayça Çesmelioglu. On some permutation binomials of the form $x^{\frac{2^n-1}{k}+1} + ax$ over $\mathbb{F}_{2^n}$: Existence and count. In *Arithmetic of Finite Fields - 4th International*

Workshop, WAIFI 2012, Bochum, Germany, July 16-19, 2012. Proceedings, pages 236–246, 2012.

[SV95] Claus P Schnorr and Serge Vaudenay. Black box cryptanalysis of hash networks based on multipermutations. In *Advances in Cryptology—EUROCRYPT'94*, pages 47–57. Springer, 1995.

[Sch96] Ralph-Hardo Schulz. Check character systems over groups and orthogonal latin squares. *Applicable Algebra in Engineering, Communication and Computing*, 7(2):125–132, 1996.

[SW10] Rasha Shaheen and Arne Winterhof. Permutations of finite fields for check digit systems. *Designs, Codes and Cryptography*, 57(3):361–371, 2010.

[Shp92a] Igor E Shparlinski. *Computational and algorithmic problems in finite fields*, volume 88. Springer Science & Business Media, 1992.

[Shp92b] Igor E Shparlinski. A deterministic test for permutation polynomials. *Computational complexity*, 2(2):129–132, 1992.

[Sma91] Charles Small. *Arithmetic of finite fields*, volume 148. CRC Press, 1991.

[TZH14] Ziran Tu, Xiangyong Zeng, and Lei Hu. Several classes of complete permutation polynomials. *Finite Fields and Their Applications*, 25(0):182 – 193, 2014.

[TZHL13] Ziran Tu, Xiangyong Zeng, Lei Hu, and Chunlei Li. A class of binomial permutation polynomials. *CoRR*, abs/1310.0337, 2013.

[Tur88] Gerhard Turnwald. Permutation polynomials of binomial type. *Contributions to general algebra*, 6:281–286, 1988.

[Tur95] Gerhard Turnwald. A new criterion for permutation polynomials. *Finite Fields and Their Applications*, 1(1):64–82, 1995.

[Vau74] Theresa P. Vaughn. Polynomials and linear transformations over finite fields. *Journal für die reine und angewandte Mathematik*, 267:179–206, 1974.

[vzG91] Joachim von zur Gathen. Values of polynomials over finite fields. *Bulletin of the Australian Mathematical Society*, 43(01):141–146, 1991.

[vzGG13] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge university press, 2013.

[Wan93] D Wan. A generalization of the carlitz conjecture. *Finite Fields, Coding Theory and Advances in Communications and Computing, Lecture Notes in Pure and Applied Mathematics, Dekker*, 141:431–432, 1993.

[Wan87] Daqing Wan. Permutation polynomials over finite fields. *Acta Mathematica Sinica*, 3(1):1–5, 1987.

[Wan92] Daqing Wan. A p-adic lifting lemma and its application to permutation polynomials. In *Finite Fields, Coding Theory, and Advances in Communications and Computing*, volume 141 of *Lecture Notes in Pure and Applied Mathematics*, pages 209–216. Marcel Dekker, New York, 1992.

[WMS95] Daqing Wan, Gary L Mullen, and Peter Jau-Shyong Shiue. The number of permutation polynomials of the form $f(x) + cx$ over a finite field. *Proceedings of the Edinburgh Mathematical Society (Series 2)*, 38(01):133–149, 1995.

[Wan02] Luyan Wang. On permutation polynomials. *Finite Fields and Their Applications*, 8(3):311 – 322, 2002.

[Wan07] Qiang Wang. Cyclotomic mapping permutation polynomials over finite fields. In *Sequences, Subsequences, and Consequences*, pages 119–128. Springer, 2007.

[Wan13] Qiang Wang. Cyclotomy and permutation polynomials of large indices. *Finite Fields and Their Applications*, 22:57–69, 2013.

[Win14] Arne Winterhof. Generalizations of complete mappings of finite fields and some applications. *Journal of Symbolic Computation*, 64:42–52, 2014.

[WLHZ14] Gaofei Wu, Nian Li, Tor Helleseth, and Yuqing Zhang. Some classes of monomial complete permutation polynomials over finite fields of characteristic two. *Finite Fields and Their Applications*, 28:148–165, 2014.

[WLHZ15] GaoFei Wu, Nian Li, Tor Helleseth, and YuQing Zhang. Some classes of complete permutation polynomials over $\mathbb{F}_q$. *Science China Mathematics*, pages 1–14, 2015.

[Zie09] Michael Zieve. On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{\frac{q-1}{d}})$. *Proceedings of the American Mathematical Society*, 137(7):2209–2216, 2009.

[Zie13] Michael Zieve. Permutation polynomials on $\mathbb{F}_q$ induced from bijective redei functions on subgroups of the multiplicative group of $\mathbb{F}_q$. *CoRR*, abs/1310.0776, 2013.

[Zie08] Michael E Zieve. Some families of permutation polynomials over finite fields. *International Journal of Number Theory*, 4(05):851–857,

2008.

[Zie10] Michael E Zieve. Classes of permutation polynomials based on cyclotomy and an additive analogue. In *Additive Number Theory*, pages 355–361. Springer, 2010.

[Zie13] Michael E. Zieve. Permutation polynomials induced from permutations of subfields, and some complete sets of mutually orthogonal latin squares. *CoRR*, abs/1312.1325, 2013.