REPORTS
IN
INFORMATICS

ISSN 0333-3590

Asymptotic Overview on Separating Codes

Gerard D. Cohen
Hans Georg Schaathun

REPORT NO 248 **May 2003**

Department of Informatics

UNIVERSITY OF BERGEN

Bergen, Norway

This report has URL
http://www.ii.uib.no/publikasjoner/texrap/ps/2003-248.ps

Reports in Informatics from Department of Informatics, University of Bergen, Norway,
is available at http://www.ii.uib.no/publikasjoner/texrap/.

Requests for paper copies of this report can be sent to:

Department of Informatics, University of Bergen, Høyteknologisenteret,
P.O. Box 7800, N-5020 Bergen, Norway

Asymptotic Overview on Separating Codes

Gérard D. Cohen	Hans Georg Schaathun
ENST Dept. INFRES	UiB Dept. of informatics
46, rue Barrault	Høyteknologisenteret
F-75634 Paris Cedex 13	N-5020 Bergen
France	Norway
cohen@enst.fr	georg@ii.uib.no

5th May 2003

Abstract

Separating codes (or systems) are known from combinatorics, and they enjoy increasing attention due to applications in digital fingerprinting. Previous applications are found in automata theory and the construction of fault-tolerant systems.

Let Γ be a code of length n, and (T, U) a pair of disjoint subsets of Γ. We say that (T, U) is separated if there exists a coordinate i, such that for any codeword $(c_1, \ldots, c_n) \in T$ and any codeword $(c'_1, \ldots, c'_n) \in U$, $c_i \neq c'_i$. The code Γ is (t, u)-separating if all pairs (T, U) with $\#T = t$ and $\#U = u$ are separated.

In this report, we give an overview of existing techniques for bounding the asymptotical rate of separating codes, including some constructions and construction techniques. We provide numerical results for binary (t, u)-separating codes for some small values of t and u. The report includes both old and new results.

Keywords
separating system, intersecting code

Synthèse asymptotique sur les codes séparants

Résumé

Les codes, ou systèmes, séparants sont connus en Combinatoire ; ils ont été utilisés, sous des vocables divers, dans des problèmes de tatouage numérique. Les premières utilisations de ce concept remontent à la théorie des automates et aux systèmes tolérant les fautes.

Soit Γ un code de longeur n, et (T, U) un couple de sous-ensembles disjoints de Γ. On dit que (T, U) est séparé s'il existe une position i telle que pour tout mot $(c_1, \ldots, c_n) \in T$ et tout mot $(c'_1, \ldots, c'_n) \in U$, $c_i \neq c'_i$. Le code Γ est dit (t, u)-séparant si tout tel couple où $\#T = t$ et $\#U = u$ est séparé.

Nous présentons de nouvelles et d'anciennes bornes, des généralisations et des constructions de codes séparants. Nous fournissons des résultats numériques pour les petites valeurs de t et u.

Mots-clefs

système séparant, code intersectant

Asymptotisk oversyn over skiljande kodar

Samandrag

Me kjenner skiljande kodar frå kombinatorikken. I dei siste åra har dei dukka opp i samband med digital fingerprenting. Andre bruksområde er i autamatateori og konstruksjon av feil-tolerante system.

Lat Γ vera ein kode med lengd n, og lat (T, U) vera eit par av disjunkte delmengder av Γ. Me seier at (T, U) er skilt dersom det er ein plass i slik at for alle ord $(c_1, \ldots, c_n) \in T$ og alle ord $(c'_1, \ldots, c'_n) \in U$, har me $c_i \neq c'_i$. Koden Γ er skiljande om alle slike par med $\#T = t$ og $\#U = u$ er skilde.

Rapporten gjev eit oversyn over kjende teknikkar for å finna skrankar for den asymptotiske raten til skiljande kodar. Me får og med eit par eksplisitte konstruksjonar, og me gjev numeriske resultat for binære (t, u)-skiljande kodar for somme små verdiar av t og u. Rapporten omfattar både nye og gamle resultat.

Stikkord

skiljande system, snittande kode

Contents

List of Tables

Preface

A couple of years ago, we wrote a report on separating codes [CES01]. During the time that has passed, several new results have emerged. This report is an update of the previous one, including the results we have published in [CES02, CELS01, CS03b, CS03a]. We also present some new results which we hope to publish in the near future.

It must also be mentioned that some errors has been found in [CES01]. Theorem 9 is somewhat weaker than the corresponding, incorrect propositions in [CES01] and [CELS01]. In addition there were a few misprints, which have been corrected, particularly the best constructible rate of $(3, 1)$- and $(3, 3)$-SS (in Table 5.1 in the old version).

Chapter 1

Introduction

The theory of separating systems has been applied in different areas of science and technology such as automata synthesis, technical diagnosis, constructions of hash functions, and authenticating ownership claims. We will make a formal and general definition in the next chapter. Separating systems is a combinatorial concept, which have been described in different frameworks and languages, some of which we are going to exemplify in the introduction.

The case of $(2,2)$-separation is introduced by Sagalovich in the context of automata: two such systems transiting simultaneously from state a to a' and from b to b' respectively should be forbidden to pass through a common intermediate state. A state of the system in this case is an n-bit binary string, and the moving from one state to another is obtained by flipping bits one by one. Only shortest paths from the old to the new state are allowed, so moving from a to a' will only involve flipping bits where a and a' differ. The set of valid states Γ forms a $(2,2)$-separating system, if for any four distinct states, a, a', b, and b' from Γ, the transitions $a \to a'$ and $b \to b'$ cannot pass through any common state. Sagalovich's contribution on this topic is substantial, e.g. [Sag65, Sag75]; a fairly recent survey can be found in [Sag94].

The recent interest in separating codes comes mainly from digital fingerprinting [BS98]. A vendor distributes digital copies of a copyrighted work, and she wants to prevent the users from making illegal copies. A digital watermark is a perceptually invisible pattern embedded in a digital file. Watermarking can be used to give every sold copy a unique ID, a digital fingerprint, identifying the buyer. If an illegal copy subsequently appears, the user guilty of copying may be identified and prosecuted.

An interesting combinatorial problem arise in the venture to protect against coalitions of pirates. If several users collude, they may compare their copies, and every differing bit must be part of the fingerprint. Thus having identified part of the fingerprint, the pirates may also change it and produce illegal copies with invalid fingerprint. The fingerprints the pirates are able to forge form the so-called feasible set, defined as

$$F(T) := \{(v_1, \dots, v_n) \in Q^n \mid \forall i, 1 \le i \le n, \exists (a_1, \dots, a_n) \in T, a_i = v_i\},$$

where T is the set of fingerprints held by the pirates, Q is the alphabet, and n is the length of a fingerprint.

If the set (code) of valid fingerprints still makes it possible to trace at least one guilty pirate out of a coalition of size t or less, we say that the code has the t-identifiable parent property (t-IPP). If the pirates are able to forge the fingerprint of an innocent user, we say that this user is framed. Codes which prevent framing are called frameproof codes, and this concept coïncides with $(t, 1)$-separation. Other kinds of separating codes have also been used to construct IPP codes [BCE+01, BBK01a, BBK01b]. In [Sch03] it was proved that good $(2, 2)$-separating codes are also 2-IPP.

The design of self-checking asynchronous networks has been a challenging problem. Friedmann et al. [FGU69] have shown that the unicode single-transition-time asynchronous state assignment correspond to $(2, 2)$- and $(2, 1)$-separating systems. The coding problem for automata states also motivated research on $(3, 3)$-SS [Ung69].

Separating codes have also been studied in a set theoretic framework, e.g. [KS88], and Körner [Kör95] gives a series of problems equivalent to $(2, 1)$-separating codes.

The outlay of the report is as follows. Chapter 2 gives the background and basic preliminaries for the study. Chapters 3-6 survey the available techniques for bounding the asymptotic rate of separating codes. We make some generalisations and improvements on former results, but in essence this techniques are known, or even well-known. Tables of best known bounds in the binary case are presented in Chapters 7 and 8.

Chapter 2

Preliminaries

There are a few properties which may be covered by our general definition of separating systems. The most well-known of these is probably z-hashing families [BW98], but there is also a substantial literature on (t,u)-separating systems. A couple of years ago, (a,b)-partial hashing was introduced [BCE+01]. When we define $(t_1,\ldots,t_z)$-separating systems, we cover all of this: for $z = 2$ we have the (t,u)-separation known from [FGU69]; when $t_i = 1$ for each i, we have z-hashing; and when $z = a+1$, $t_z = b-a$, and $t_i = 1$ for $i < z$, we have (a,b)-partial hashing.

First let us agree on some standard notation. Let Q be an additive group (often a field) called the alphabet, and denote by q its number of elements. Let $\mathbb{V}$ be the set of n-tuples over Q. An $(n,M)_q$ code Γ is an M-subset $\Gamma \subseteq \mathbb{V}$. If Q is a field of q elements and C is a k-dimensional subspace $C \leqq \mathbb{V}$, then we say that C is a $[n,k]_q$ (linear) code. We will refer to the elements of $\mathbb{V}$ as words.

Definition 1
A sequence $(T_1,\ldots,T_z)$ of pairwise disjoint sets of words is called a $(t_1,\ldots,t_z)$-configuration if $\#T_j = t_j$ for all j. Such a configuration is separated if there is a position i, such that for all $l \neq l'$ every word of T_l is different from every word of $T_{l'}$ on position i.

A code is $(t_1,\ldots,t_z)$-separating if every $(t_1,\ldots,t_z)$-configuration is separated. A $\mathbf{t}$-separating code is also called a $\mathbf{t}$-SS (separating system).

In earlier works on watermarking, (t,t)-separating codes have been called t-PIC (partially identifying codes) [CE00b] or t-SFP (secure frameproof) [SW98, SvTW00, SSW00]. The current terminology appears to be older though [Sag94]. Different special cases have also appeared in literature; the t-frameproof codes from [SSW00] are just $(t,1)$-separating codes.

In the literature, the binary alphabet is dominant. An extensive study of $(2,1)$-SS is found in [Kör95]. Apparently, the notions of non-binary $(2,1)$- and $(2,2)$-SS were introduced in [Sag82], but the concept had been studied in [PS72, Sag73, Sag75] under different names.

2.1 Basic definitions

For any word $\mathbf{c} = (c_1, \dots, c_n) \in \mathbb{V}$ we define the support to be

$$\chi(\mathbf{c}) := \{i \mid c_i \neq 0\}.$$

For any subset $S \subseteq \mathbb{V}$, the support is

$$\chi(S) := \bigcup_{\mathbf{c} \in S} \chi(\mathbf{c}).$$

We define the weight of subsets and codewords to be the size of their support, and denote it $w(\mathbf{c}) := \#\chi(\mathbf{c})$ or $w(S) := \#\chi(S)$.

Let C be a linear code. The r-th minimum support weight d_r of C is the least weight of an r-dimensional subcode of C. The r-th maximum support weight m_r is the largest weight of an r-dimensional subcode of C. Both these numbers were first studied in [HKM77], and the minimum support weight has received quite some attention following [Wei91], where it was called the r-th generalised Hamming weight.

It is clear that d_1 is the minimum distance of the code, and likewise m_1 is the maximum distance of the code; so these two numbers are defined also for non-linear codes. Several general definitions of d_r exist for non-linear codes, but we will not need any of them here.

We write $\mathbf{t} = (t_1, \dots, t_z)$. Given a $\mathbf{t}$-configuration $(T_1, \dots, T_z)$, we define the separating set $\Theta(T_1, \dots, T_z)$ to be the set of coordinate positions where $(T_1, \dots, T_z)$ is separated. Let $\theta(T_1, \dots, T_z) := \#\Theta(T_1, \dots, T_z)$ be the separating weight. Clearly $\theta(T_1, \dots, T_z) \geq 1$ is equivalent with $(T_1, \dots, T_z)$ being separated. The minimum $\mathbf{t}$-separating weight $\theta_{\mathbf{t}}(C)$ is the least separating weight of any $\mathbf{t}$-configuration of C. The minimum separating weights have previously been studied by Sagalovich [Sag94]. Clearly $\theta_{1,1}(C) = d_1(C)$.

By an automorphism on $\mathbb{V}$, we shall understand any composition of permutations of coordinate positions and alphabet permutations in individual positions. These are exactly the maps which define equivalence classes of non-linear codes in coding theory.

Remark 2.1
If $\pi : \mathbb{V} \to \mathbb{V}$ is an automorphism, then $\theta(T_1, \dots, T_z)) = \theta(\pi(T_1), \dots, \pi(T_z))$ for any $\mathbf{t}$-configuration $(T_1, \dots, T_z)$. It follows that $\theta_{\mathbf{t}}$ is invariant over the ensemble of equivalent codes.

2.2 Basic results

Define

$$P(t_1,\dots,t_z) := \sum_{i=1}^{z-1}\sum_{j=i+1}^{z} t_i t_j.$$

Note that if $t_j = 1$ for all j, then

$$P(t_1,\dots,t_z) = \binom{z}{2},$$

and if $z = 2$, then $P(t_1,t_2) = t_1 t_2$. The following proposition generalises the results on separating codes and perfect hashing families from [SWZ00, Alo86].

Proposition 1
Any $(n,M,d)_q$ code Γ has

$$\theta_{\mathbf{t}} \geq n - P(\mathbf{t})(n-d).$$

Corollary 1
An $(n,M,d)_q$ code Γ is **t***-separating if*

$$\frac{d}{n} > 1 - \frac{1}{P(\mathbf{t})}.$$

Proof: Consider any **t**-configuration $(T_1,\dots,T_z)$ from Γ, and define the sum

$$\Sigma := \sum_{i=1}^{z-1}\sum_{j=i+1}^{z}\sum_{(x,y)\in T_i\times T_j} d(x,y).$$

This is the sum of $P(t_1,\dots,t_z)$ distances in the code, so

$$\Sigma \geq P(t_1,\dots,t_z)d. \tag{2.1}$$

Each coordinate can contribute at most $P(t_1,\dots,t_z)$ to the sum Σ, but if any coordinate does contribute that much, then the configuration is separated on this coordinate. Hence we get that

$$\Sigma \leq n(P(\mathbf{t})-1) + \theta_{\mathbf{t}}. \tag{2.2}$$

The proposition follows by combining the upper and lower bounds (2.1) and (2.2), and simplifying. □

It must be noted that, to get infinite families of separating codes with good rate, the alphabet size q grows extremely rapidly in the t_j-s, due to the Plotkin bound. On the other hand, for sufficiently large alphabets, good separating codes are constructible from algebraic geometry. We will use the following lemma by Tsfasman [Tsf91] extensively throughout the report.

Theorem 1 (The Tsfasman Codes)
For any $\alpha > 0$ there are constructible, infinite families of codes $\mathfrak{A}(N)$ with parameters $[N, NR, N\delta]_q$ for $N \geq N_0(\alpha)$ and

$$R + \delta \geq 1 - (\sqrt{q} - 1)^{-1} - \alpha.$$

Infinite families of separating codes over small alphabets can be built by concatenation. Though this construction is well-known in various special cases from the literature [Alo86], we have not found as general a statement as the one we give below. The outer codes for concatenation will very often be Tsfasman codes.

Definition 2 (Concatenation)
Let C_1 be a $(n_1, Q)_q$ and let C_2 be an $(n_2, M)_Q$ code. Then the concatenated code $C_1 \circ C_2$ is the $(n_1 n_2, M)_q$ code obtained by taking the words of C_2 and mapping every symbol on a word from C_1.

Proposition 2
Let Γ_1 be a $(n_1, M)_{M'}$ code with minimum $\mathbf{t}$-separating weight $\theta_{\mathbf{t}}^{(1)}$, and let Γ_2 be a $(n_2, M')_q$ code with separating weight $\theta_{\mathbf{t}}^{(1)}$. Then the concatenated code $\Gamma := \Gamma_2 \circ \Gamma_1$ has minimum separating weight $\theta_{\mathbf{t}} = \theta_{\mathbf{t}}^{(1)} \cdot \theta_{\mathbf{t}}^{(2)}$.

Proof: Consider a $\mathbf{t}$-configuration $(T_1, \ldots, T_z)$ in Γ. Then there is a corresponding configuration in Γ_1, $(T_1'', \ldots, T_z'')$ which is separated on a set I of at least $\theta_{\mathbf{t}}^{(1)}$ positions by assumption. Considering only the positions of Γ corresponding to a particular position $i \in I$ in Γ_2, we get a $\mathbf{t}'$-configuration $(T_1', \ldots, T_z')$ in Γ_1 where $1 \leq t_j' \leq t_j$ for all j. Clearly, $(T_1', \ldots, T_z')$ must be separated on at least $\theta_{\mathbf{t}}^{(2)}$ positions, and consequently $\theta(T_1, \ldots, T_z) \geq \theta_{\mathbf{t}}^{(1)} \theta_{\mathbf{t}}^{(2)}$, and the proposition follows. □

Note that Γ will usually not satisfy the requirements of Proposition 1. We will give a thorough example of the concatenation technique in Section 2.3.

It is easy to verify that $q \geq z$ for any $\mathbf{t}$-separating code; the alphabet must have a distinct symbol for each of the z subsets to be separated. The following proposition strengthens this result.

Proposition 3
If C is a linear, $(t_1, \ldots, t_z)$-separating code and $z \geq 3$, then $\sum_{j=1}^{z} t_j \leq q$.

Proof: First we prove that $t_1 + t_2 < q$, for if

$$T_1 \cup T_2 \supseteq \{\alpha \mathbf{c} \mid \alpha \in \mathsf{GF}(q)\},$$

then no third set T_3 will be separated from T_1 and T_2.

Let $\alpha_0, \alpha_1, \ldots, \alpha_{q-1}$ be all the field elements, where $\alpha_0 = 0$ and $\alpha_1 = 1$. Let $\mathbf{a}$ and $\mathbf{b}$ be two independent codewords. Let

$$T_1 := \{\alpha_0\mathbf{a}, \ldots, \alpha_{t_1-1}\mathbf{a}\},$$
$$T_2 := \{\alpha_{t_1}\mathbf{a}, \ldots, \alpha_{t_1+t_2-1}\mathbf{a}\},$$

and let $T_3, \ldots, T_z$ be any sequence of pairwise disjoint sets such that

$$T := \bigcup_{j=3}^{z} T_j = \{\mathbf{a} + \alpha_1\mathbf{b}, \ldots, \mathbf{a} + \alpha_{t'}\mathbf{b}\},$$

where $t' = t_3 + \ldots + t_z$. Clearly, T_1 and T_2 are only separated on $\chi(\mathbf{a})$. Also T and T_1 are only separated on $\chi(\mathbf{b})$. On any coordinate $i \in \chi(\mathbf{a}) \cap \chi(\mathbf{b})$, $t_1 + t_2$ different values occur in $T_1 \cup T_2$ and t' different values occur in T. Hence the configuration can only be separated if

$$t' + t_1 + t_2 = t_1 + \ldots + t_z \leq q,$$

as required. □

Corollary 2
If C is a linear q-ary, (t,u)-partially hashing code with $t \geq 2$, then $u \leq q$.

These bounds are tight, since q-hashing codes can be constructed for any q.

Proposition 4
Let $\mathbf{a}$ and $\mathbf{b}$ be two linearly independent codewords, and write $T = \{\mathbf{a}, \mathbf{b} + \alpha\mathbf{a} \mid \alpha \in \mathsf{GF}(q)\}$. Then $(\mathbf{0}, T)$ is a $(q+1, 1)$-configuration which is not separated.

Proof: We shall prove that in every position i, at least one codeword in T has a 0. If $b_i = 0$, this holds, so assume $b_i \neq 0$. Then $\mathbf{b} + (-a_i^{-1})b_i\mathbf{a}$ has 0 in position i, as required. □

Corollary 3
If C is q-ary, linear (t,t')-separating, then $\max\{t,t'\} \leq q$.

This bound is tight in the binary case, since $(2,2)$-separating, binary, linear codes are known to exist (e.g. [Sag94]).

Theorem 2
If C is a non-binary, linear (t,t')-separating, then $t + t' \leq q + 1$.

Proof: We have already proved that $t, t' \leq q$. It only remains to prove that we can construct a non-separated $(t, q+2-t)$-configuration for all t such that $2 \leq t \leq q$. Let $\alpha_0, \alpha_1, \ldots, \alpha_{q-1}$ be all the fields elements, where $\alpha_0 = 0$ and $\alpha_1 = 1$. Let $\mathbf{a}$ and $\mathbf{b}$ be two independent codewords. A non-separated $(t, q+2-t)$-configuration is given by

$$(\{\alpha_0\mathbf{a}, \ldots, \alpha_{t-1}\mathbf{a}\}, \{\alpha_t\mathbf{a}, \mathbf{a}+\alpha_1\mathbf{b}, \ldots, \mathbf{a}+\alpha_{q+1-t}\mathbf{b}\}).$$

First note that $\alpha_t\mathbf{a}$ matches $\mathbf{0}$ on every position not in $\chi(\mathbf{a})$, and $\mathbf{a}+\mathbf{b}$ match $\mathbf{a}$ on every position not in $\chi(\mathbf{b})$. In every position in $\chi(\mathbf{a}) \cap \chi(\mathbf{b})$, we get t different field values in the first set, and $q+1-t$ different field values from the $\mathbf{a}+\alpha_i\mathbf{b}$. Since there are only q elements in the field, they cannot be separated. $\square$

2.3 The tetracode and compositions thereof

The ternary constructions will make use of three ingredient codes, and apply twice the concatenation method. We will obtain an asymptotic code which is $(2,2)$-, $(3,1)$-, and $(1,1,1)$-separating. Recall that no stronger separating properties is possible for a ternary code, by Theorem 2 and Corollary 3.

The first seed is the remarkable $[4,2,3]_3$ tetracode $\mathfrak{T}$, defined by the generator matrix

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{bmatrix}.$$

This code is self-dual and MDS (on Singleton's bound $d = n-k+1$). It is both an extended perfect Hamming code and a simplex (all codewords are at distance 3 apart). Thus it follows that $\mathfrak{T}$ is 3-hashing and $(3,1)$-separating from Proposition 1. Furthermore, it is $(2,2)$-separating by Theorem 19. The tetracode was proved 3-hashing in [KM88], and it was proved to have the IPP property in [HvLLT98].

Let $\mathfrak{R}_1$ be the $[9,3,7]_{3^2}$ Reed-Solomon code, which is both $(2,2)$- and $(1,3)$-separating, and 3-hashing by Proposition 1. The concatenated code $\mathfrak{T} \circ \mathfrak{R}_1$ has parameters $[36,6]_3$, and by Proposition 2, it is $(2,2)$- and $(1,3)$-separating, and 3-hashing. With 3^6 codewords, this code can be concatenated with $\mathfrak{A}(N)$ over $\mathsf{GF}(3^6)$ which gives a reasonable rate.

The concatenated code $\mathfrak{T} \circ \mathfrak{R}_1 \circ \mathfrak{A}(N)$ gives an infinite family of linear, ternary $(3,1)$- and $(2,2)$-separating and 3-hashing codes with rate $R'/6 \approx 0.0352$.

If we only want $(3,1)$-separating and 3-hashing codes, we can obtain a better rate by using the Reed-Solomon code $\mathfrak{R}_2$ with parameters $[10,4,7]_{3^2}$, which results in the concatenated code $\mathfrak{T} \circ \mathfrak{R}_2$ with parameters $[40,8]_3$. Then we take the infinite family $\mathfrak{A}(N)$ of codes with parameters $[N, K, D = \lceil 2N/3 \rceil + 1]_{3^8}$ of rate

$1/3-(3^4-1)^{-1}$, and the concatenated code $\mathfrak{T}\circ\mathfrak{R}_2\circ\mathfrak{A}(N)$ is an infinite family of linear ternary $(3,1)$-separating and 3-hashing codes with rate approximately $77/1200 \approx 0.0642$.

Example 2.1 *We sketch a construction with $q = 4$ as well. As in the previous example, we concatenate three codes to build the infinite family. Each code has $d/n > 3/4$ and thus is $(2,2)$-separating by Proposition 1. The first two are doubly extended Reed-Solomon codes. We take successively:*

1. $C_1[5,2,4]_4$;
2. $C_2[17,5,13]_{4^2}$, *getting* $C_1 \circ C_2[85,10]_4$;
3. *and finally,* $C(N)[N,K,D = \lceil 3N/4\rceil + 1]_{4^{10}}$ *with rate* $\approx 1/4-(4^5-1)^{-1} \approx 1/4$.

The final outcome is an infinite constructive family of linear quaternary $(2,2)$-separating codes with rate approximately $1/34 \approx 0.029$.

Chapter 3

On $(t, 1)$-separating codes

In this chapter we prove an upper bound on $(t, 1)$-SS. Interestingly enough, this bound is independent of the alphabet size q.

A (t, τ)-cover free code is a code with $(t, 1)$-separating weight at least equal to τ. Such codes were studied in [GSW00] and [KRS99] motivated by broadcast encryption. The results in this chapter were also presented in [CS03a].

Partition $\{1, 2, ..n\}$ into t almost equal parts $P_1, \ldots, P_t$ of size approximately n/t. Say a codeword c is *isolated* on P_i if no other codeword projects onto a n/t-tuple on P_i located at distance less than $(n/t)\tau$ from c. Denote by U_i the subset of codewords isolated on P_i.

Lemma 1
If C is (t, τ)-cover free, then every codeword c of C is isolated on at least one P_i.

Proof: Suppose for a contradiction that there is a codeword $\mathbf{c}_0$ which is not isolated. Let $\mathbf{c}_i$ be a codeword which is at distance less than $(n/t)\tau$ when projected onto P_i, for $i = 1, \ldots, t$. Now $\mathbf{c}_0$ is separated from $\{\mathbf{c}_1, \ldots, \mathbf{c}_t\}$ on less than $(n/t)\tau$ coordinates per block, or at most $n\tau - t$ coordinate positions total. This contradicts the assumption on the separating weight τ. $\square$

If we let τ tend to zero, we get an upper bound on $(t, 1)$-SS, which was found independently in [CS03b] and [Bla03b]. The proofs are essentially the same as the one presented here.

Theorem 3
If C is (t, τ)-cover free, then $|C| \le tq^{\lceil (1-\tau)n/t \rceil}$.

For constant t, this asymptotically gives $R \le (1 - \tau)/t$ when n increases. This rate is obtained by the Tsfasman codes (Theorem 1) by Proposition 1, when $\delta > t^{-1}(1 - \tau)$. The lower bound for arbitrary q has been studied in more detail in [Xin02].

Theorem 4
For fixed t and large enough q, the largest possible rate of a q-ary family of (t,τ)-cover free codes satisfies $R = t^{-1}(1-\tau)(1+o(1))$.

Chapter 4

Upper bounds by projection

In this chapter we shall give a general presentation of the well-known projection arguments for upper bounds. The technique have been used for decades, but the results have continuously been refined in various ways, see e.g. [Sag94]. The latest refinements for binary (t,t)-SS appeared in [CS03b].

4.1 Stronger properties in the binary case

Separating codes are related to two stronger concepts. Completely separating codes ((t,t')-CSS) are used in automata theory and fault-tolerant systems alongside the separating codes. Superimposed codes ((t,t')-SI) where introduced in [KS64], and have been studied in several papers, e.g. [DR83, DVMT02].

We will consider the binary case only. Consider any $t+t'$ codewords and view them as rows of a matrix. If the code is separating, there must be at least one so-called regular column, which is either $\mathbf{x}_0 = (0\dots01\dots1)$ with t zeroes and t' ones, or $\mathbf{x}_1 = (1\dots10\dots0)$ with t ones and t' zeroes.

If the code is (t,t')-superimposed, we demand at least one column of type $\mathbf{x}_0$, and if the code is (t,t')-completely separating, we demand both $\mathbf{x}_1$ and $\mathbf{x}_0$. Thus separating codes is clearly the weakest concept, while completely separating systems is the strongest. If $t = t'$, superimposed codes and completely separating codes are equivalent, since the property has to hold for any ordering of the words.

Let $R^{\mathrm{CSS}}(t,t')$, $R^{\mathrm{SI}}(t,t')$, and $R^{\mathrm{SS}}(t,t')$ be the best possible asymptotic rates of (t,t')-CSS, (t,t')-SI, and (t,t')-SS, respectively. Clearly we have

$$R^{\mathrm{SS}}(t,t') \geq R^{\mathrm{SI}}(t,t') \geq R^{\mathrm{CSS}}(t,t') \geq \frac{1}{2}R^{\mathrm{SS}}(t,t').$$

We denote by $\bar{R}^x(t,t')$ any upper bound on $R^x(t,t')$. Let $\bar{R}(\delta)$ be any upper bound on the asymptotic rate of error-correcting codes with normalised minimum distance δ.

4.2 Improved upper bounds on (t,t')-SS

Proposition 5
Any binary (t,u)-separating $(\theta_{0,0}, M, \theta_{1,1})$ code Γ with separating weights $\theta_{a,b}$, for $1 \le a \le t$ and $1 \le b \le u$, gives rise to, for any positive $v < \min\{t,u\}$, a completely $(t-v,u-v)$-separating $(\theta_{v,v}, M-2v, 2\theta_{v+1,v+1})$ code Γ' with complete-separating weight $\theta'_{a,b} = \theta_{a+v,u+v}$ for $1 \le a \le t-v$ and $1 \le b \le u-v$.

Proof: Consider two v-tuples V and V' of words from Γ, such that they have separating weight $\theta_{v,v}$. Assume by translation that (V,V') has $\theta_{v,v}$ columns of the form $(0\dots01\dots1)$. Let Γ' be the code obtained from Γ by deleting every column where (V,V') is not separated and the $2v$ words from V and V'. Clearly Γ' has the length and dimension claimed by the proposition. It remains to prove the separating weights.

Let (T,U) be a (t',u')-configuration from Γ where $t' \le t-v$ and $u' \le u-v$). Then both $(V \cup T, V' \cup U)$ and $(V' \cup T, V \cup U)$ must have separating weight at least $\theta_{t'+v,u'+v}$, which implies that (T,U) is completely separated with weight at least $\theta_{t'+v,u'+v}$. This holds even when restricting only to the positions where (V,V') is separated. □

The following proposition is proved in the same way.

Proposition 6
Any completely (t,u)-separating $(n,M,2\theta_{1,1})$ code with completely separating weights $\theta_{a,b}$, for $1 \le a \le t$ and $1 \le b \le u$, gives rise to, for any positive $v < \min\{t,u\}$, a completely $(t-v,u-v)$-separating $(\theta_{v,v}, M-2v, 2\theta_{v+1,v+1})$ code with complete-separating weight $\theta'_{a,b} = \theta_{a+v,u+v}$ for $1 \le a \le t-v$ and $1 \le b \le u-v$.

Theorem 5
We have for $t,u \ge 2$ that

$$R^{\mathrm{CSS}}(t,u) \le \bar{R}\Big(\frac{2R^{\mathrm{CSS}}(t,u)}{\bar{R}^{\mathrm{CSS}}(t-1,u-1)}\Big),$$
$$R^{\mathrm{SS}}(t,u) \le \bar{R}\Big(\frac{R^{\mathrm{SS}}(t,u)}{\bar{R}^{\mathrm{CSS}}(t-1,u-1)}\Big).$$

Proof: Let C be a (t,u)-CSS with rate $R = R^{\mathrm{CSS}}(t,u)$, and let C' be the $(t-1,u-1)$-CSS which exists by Proposition 6. Denote by R' the rate of C'. We have that

$$\delta = 2\frac{\theta_{1,1}}{\theta_{0,0}} = 2\frac{\log M}{\theta_{0,0}}\frac{\theta_{1,1}}{\log M} = 2R/R'.$$

Now, obviously $R \le \bar{R}(\delta)$, which is decreasing in δ_t, and this gives the result. The bound on R^{SS} is similar, except that the minimum distance of C is $d = \theta_{1,1}$ instead of $2\theta_{1,1}$. □

(t,t')	CSS	SIC	SS
$(2,1)$	—	0.3219[2]	0.5[1]
$(3,1)$	—	0.1993[2]	0.3333[1]
$(3,2)$	0.06627	0.07449[3]	0.1202
$(4,2)$	0.04301	0.04552[3]	0.07994
$(4,3)$	0.01533	0.01828[3]	0.02951

[1] Theorem 3
[2] [DVMT02]
[3] [KLO03]

(t,t)	CSS	SS
$(1,1)$	1.0000	1.0000
$(2,2)$	0.1610[2]	0.2835
$(3,3)$	0.03534	0.06627
$(4,4)$	0.008368	0.01630
$(5,5)$	0.002042	0.004037

Table 4.1: Upper bounds on completely separating codes (CSS), superimposed codes (SIC), and separating codes (SS) over a binary alphabet.

This theorem provides a recursive bound on separating codes. The general idea is not new, at least the derived bound on $(2,2)$-SS has been known for ages, see [Sag94]. Even so, the results we obtain here for (t,t)-CSS are stronger than those recently presented in [DVMT02] (except for $t = 2$).

We use the McEliece-Rodemich-Rumsey-Welch bound for $\bar{R}(\delta)$, as given in the following theorem. See [Aal90, Lev98] for the non-binary form and [MRRW77, MS77] for the original (binary) version.

Theorem 6 (McEliece-Rodemich-Rumsey-Welch bound)
For any (n,M,d) code, we have

$$R(\delta) \leq H_q(((q-1)-(q-2)\delta - 2\sqrt{(q-1)\delta(1-\delta)})/q),$$

where

$$H_q(x) = -(1-x)\log_q(1-x) - x\log_q x + x\log_q(q-1).$$

In Table 4.1, we summarise the rate we get for small t and t', and $q = 2$. Most of the rates are obtained by using the theorems of this chapter recursively. The first bounds in the iterations are copied from other works. Observe that we improve the bounds also on (t,t)-superimposed codes for $t \geq 3$.

Example 4.1 *Let C_1 be an asymptotic class of $(\theta_0, 2^k, \theta_1)$ $(3,3)$-SS. Then there is an asymptotic class C_2 of $(\theta_1, 2^k, \theta_2)$ $(2,2)$-CSS. We have that $R_2 = k/\theta_1 \leq 0.161$, and*

$$R_1 = k/\theta_0 = R_2\delta_1 \leq 0.161\delta_1,$$

which is equivalent to

$$\delta_1 \geq R_1/0.161.$$

We can use any upper bound $\bar{R}(\delta)$ on R_1, and get

$$R_1 \le \bar{R}(\delta_1) \le \bar{R}(R_1/0.161).$$

Using the Theorem 6, we get $R_1 \le 0.0663$.

Problem 4.1 *Make a bound on the rate for given $\tau_{t,t'}$.*

Problem 4.2 *Retrieve a proof of the bound on $(3,3)$-SS, $R \le 0.0658$ from [CGL01].*

Problem 4.3 *Is it possible to get rid of the recursion and find a simple closed form expression for the upper bound?*

4.3 Ternary bounds

In the non-binary case, complete separation is not clearly defined. When $q > 3$, we are not able to prove the recursive bound stronger than

$$R_q^{\mathrm{SS}}(t,u) \le \bar{R}\Big(\frac{R_q^{\mathrm{SS}}(t,u)}{\bar{R}_q^{\mathrm{SS}}(t-1,u-1)}\Big),$$

which is considerably weaker than the binary result. The reason for this is found in the proof of Propositions 5 and 6. Because there are four alphabet symbols (or more), it is possible to have one column which separates both $(V \cup T, V' \cup U)$ and $(V' \cup T, V \cup U)$.

In the ternary case we are able to get a strong analogue of the binary results by the definition of ternary pseudo-completely separating weight. Let (T,U) be a (t,u)-configuration. A column i is regular if it separates (T,U). A regular column i is of Type 0 if $x_i \neq 1$ for all $\mathbf{x} \in T$ and $y_i \neq 0$ for all $\mathbf{y} \in U$. It is of Type 1 if $x_i \neq 0$ for all $\mathbf{x} \in T$ and $y_i \neq 1$ for all $\mathbf{y} \in U$. Note that one column can be both of Type 1 and of Type 2 if and only if $q > 3$.

The pseudo-completely separating weight of a ternary code C is the largest number $\theta_{t,u}$ such that any (t,u)-configuration has at least $\theta_{t,u}$ regular columns of Type 0 and at least $\theta_{t,u}$ regular columns of Type 1.

The following two lemmata can be proved using the proof of Proposition 5.

Lemma 2
Any ternary (t,u)-separating $(\theta_{0,0}, M, \theta_{1,1})$ code Γ with separating weights $\theta_{a,b}$, for $1 \le a \le t$ and $1 \le b \le u$, gives rise to, for any positive $v < \min\{t,u\}$, a pseudo-completely $(t-v, u-v)$-separating $(\theta_{v,v}, M-2v, 2\theta_{v+1,v+1})$ code Γ' with pseudo-completely separating weight $\theta'_{a,b} = \theta_{a+v,u+v}$.

(t,t)	PCSS	SS
$(1,1)$	1	1
$(2,2)$	0.2197	0.3237
$(3,3)$	0.06204	0.1138
$(4,4)$	0.01913	0.03675
$(5,5)$	0.006120	0.01202

(t,t')	PCSS	SS
$(3,2)$	0.1268	0.2197
$(4,3)$	0.03751	0.07056
$(5,4)$	0.01180	0.02290
$(4,2)$	0.08978	0.1605
$(5,3)$	0.02713	0.05167
$(5,2)$	0.06966	0.1268

Table 4.2: Upper bounds on ternary separating codes, computed by using the bound $R \leq 1/t$ for $(t,1)$-SS and -PCSS (Theorem 3) and recursive application of Theorem 7.

Lemma 3
Any ternary pseudo-completely (t,u)-separating $(\theta_{0,0}, M, 2\theta_{1,1})$ code Γ with pseudo-completely separating weights $\theta_{a,b}$, for $1 \leq a \leq t$ and $1 \leq b \leq u$, gives rise to, for any positive $v < \min\{t,u\}$, a pseudo-completely $(t-v,u-v)$-separating $(\theta_{v,v}, M-2v, 2\theta_{v+1,v+1})$ code Γ' with pseudo-completely separating weight $\theta'_{a,b} = \theta_{a+v,u+v}$.

Analogously of Theorem 5, we get the following theorem. Table 4.2 follows by combining Theorem 7 with the McEliece et al. bound.

Theorem 7
We have for $t,u \geq 2$ that

$$R_3^{\mathrm{PCSS}}(t,u) \leq \bar{R}\Big(\frac{2R_3^{\mathrm{PCSS}}(t,u)}{\bar{R}_3^{\mathrm{PCSS}}(t-1,u-1)}\Big),$$
$$R_3^{\mathrm{SS}}(t,u) \leq \bar{R}\Big(\frac{R_3^{\mathrm{SS}}(t,u)}{\bar{R}_3^{\mathrm{PCSS}}(t-1,u-1)}\Big).$$

4.4 Bounds on linear separating codes

Let $R_q^{\mathrm{LSS}}(t,u)$ be the highest possible rate for an asymptotic family of linear, q-ary (t,u)-separating code.

Proposition 7
Any linear separating $[\theta_{0,0}, k, \theta_{1,1}]$ code C with separating weights $\theta_{a,b}$, where $1 \leq a \leq t$ and $1 \leq b \leq u$, gives rise to a linear separating $[\theta_{0,1}, k-1, \theta_{1,2}]$ code C' with separating weights $\theta'_{a,b} = \theta_{a,b+1}$, where $1 \leq a \leq t$ and $1 \leq b \leq u-1$.

Proof: Let $\mathbf{c} \in C$ be a codeword of weight $\theta_{1,1}$. Let C' be the code obtained by shortening C on every position where $\mathbf{c}$ is zero. It remains to prove that $\theta_{a,b}(C') \geq$

$t+u$	Rate
3	0.3537
4	0.1683
5	0.09050
6	0.05206

Table 4.3: Upper bounds on ternary linear separating codes, computed by recursive application of Corollary 4.

$\theta_{a,b+1}(C)$ for all a and b. It is sufficient that any (a,b)-configuration (A,B) of C' with $\mathbf{0} \in A$ has separating weight at least $\theta_{a,b+1}(C)$. Consider the corresponding $(a,b+1)$-configuration $(A,B') = (A,B \cup \{\mathbf{c}\})$ in C. Observe that (A,B') can only be separated where $\mathbf{c}$ is non-zero, i.e. on position existing in C'. Hence $\theta(A,B) = \theta(A,B') \geq \theta_{a,b+1}(C)$ as required. □

Corollary 4
For any $t \geq 1$ and $u \geq 2$, we have

$$R_q^{\mathrm{LSS}}(t,u) \leq \bar{R}\Big(\frac{R_q^{\mathrm{LSS}}(t,u)}{\bar{R}_q^{\mathrm{LSS}}(t,u-1)}\Big).$$

Note that this bound depends only on the sum $t+u$. We have computed numerical values for $q=3$ in Table 4.3. Applying the corollary for $q=2$ gives us the same bounds as the ones we get from intersecting codes in Chapter 5.

Chapter 5

Almost linear separating codes

We have seen that a binary, linear code cannot be more than $(2,2)$-separating. On the other hand, we know that (t,u)-separating codes can be constructed from (linear) $(t+u-1)$-wise intersecting codes by forming a non-linear subcode [CELS01]. In Section 5.2, we will present this technique, and correct some errors which unfortunately appeared in the original paper. In Section 5.1 we will present a new statement on how far from linear a (t,u)-separating code must be.

5.1 Almost linear separating codes

Theorem 8
Let C be a binary (t,u)-SS containing the zero word, and let ι be the size of the smallest set of linearly dependent non-zero words. Then we have

$$\iota > \bar{\iota}(t,u) := \begin{cases} t+u, & \text{when } t \equiv u \equiv 1 \pmod 2, \\ t+u-1, & \text{when } t \not\equiv u \pmod 2, \\ t+u-2, & \text{when } t \equiv u \equiv 0 \pmod 2. \end{cases}$$

Proof: The result is trivial for $t,u \leq 2$. We prove the lemma by induction, so assume it holds for any smaller t or u. If u or t is even, the result follows by induction because C must be $(t,u-1)$-separating and $(t-1,u)$-separating. It only remains to prove it for t and u odd.

Since C is $(t-2,u)$- and $(t,u-2)$-separating, any $t+u-2$ codewords are linearly independent by induction. Suppose there is a set $T = \{\mathbf{x}_1, \ldots, \mathbf{x}_\iota\}$ of $\iota = t+u-1$ non-zero words adding to zero. Then $(\mathbf{x}_1, \ldots, \mathbf{x}_t; \mathbf{x}_{t+1}, \ldots, \mathbf{x}_\iota, \mathbf{0})$ cannot be separated, because T cannot have an odd number of ones in any position. If $\iota = t+u$, the same argument holds for $(\mathbf{x}_1, \ldots, \mathbf{x}_t; \mathbf{x}_{t+1}, \ldots, \mathbf{x}_\iota)$. □

5.2 Intersecting codes

The first relationship between intersecting codes and separating codes appeared in [BR80]. Any linear binary $(2,1)$-SS is an intersecting code and vice versa. In this chapter we explore t-wise intersecting codes for $t \geq 3$.

Definition 3
A linear code C of dimension $k \geq t$ is said to be t-wise intersecting if any t linearly independent codewords have intersecting supports. If $t > k$, we say that C is t-wise intersecting if and only if it is k-wise intersecting.

It is easy to verify that any t-wise intersecting code is also $(t-1)$-wise intersecting.

Proposition 8
For a linear, binary code, 3-wise intersection is equivalent to $(2,2)$-separation.

The fact that linear, $(2,2)$-separating codes must be 3-wise intersecting holds not only for binary codes, and it is proved in Proposition 9 below. Unfortunately, this is the only result we have found in the non-binary case.

The fact that t-wise intersecting, binary codes gives rise to separating codes can be generalised. The statement of the proposition, will follow from the special case $t = 3, j = 2$ of Theorem 9 below.

Remark 5.1
If we have a linear, q-ary $(2,1)$-SS C, then any pair of vectors $(\mathbf{x},\mathbf{y})$ is separated from $\mathbf{0}$. Consequently $\mathbf{x}$ and $\mathbf{y}$ intersect in some position and C is 2-wise intersecting. This was observed for $q = 2$ in [BR80].

Proposition 9
Every linear $(2,2)$-separating code is 3-wise intersecting.

Proof: If $k = 2$, three-wise intersection is equivalent to 2-wise intersection according to our definition. Any $(2,2)$-separating code is $(2,1)$-separating and hence 2-wise intersecting by Remark 5.1.

Suppose C is $(2,2)$-separating, and consider three independent codewords $\mathbf{a},\mathbf{b},\mathbf{c}$. We shall prove that these three words have intersecting supports. Consider the $(2,2)$-configuration $(\mathbf{0},\mathbf{c}+\mathbf{a};\mathbf{a},\mathbf{b})$. Since C is $(2,2)$-separating, there is a position i where $\mathbf{a}$ is $\alpha \neq 0$ and $\mathbf{b}$ is $\beta \neq 0$, and $\mathbf{c}+\mathbf{a}$ is $\gamma \notin \{\alpha,\beta\}$. Now $\mathbf{c}$ is $\gamma - \alpha \neq 0$ on position i. □

Due to this proposition, we can use many bounds on separating codes as bounds on intersecting codes. For instance, by Theorem 19, every code with $4d > 3m$ is 3-wise intersecting.

Theorem 9
Let $i, j \geq 1$ be integers such that $t := i + j - 1 \geq 2$. Consider a t-wise intersecting, binary, linear code C, and a non-linear subcode $\Gamma \subseteq C$. Let $\bar{t}(i, j)$ be defined as in Theorem 8. The code Γ is (i, j)-separating if and only if any $\bar{t}(i, j)$ non-zero codewords are linearly independent.

Proof: If Γ is (i, j)-separating, then any $\bar{t}(i, j)$ codewords are independent by Theorem 8. The opposite implication is a bit tedious to prove. We start by proving that any $t+1$ codewords being linearly independent is sufficient for Γ to be (i, j)-separating. This holds as the theorem states irrespectively of the parities of i and j. Afterward we will strengthen the result in the cases where i and j are not both odd.

Choose any (two-part) sequence Y' of $t+1$ codewords from Γ,

$$Y' := (\mathbf{a}'_1, \ldots, \mathbf{a}'_j; \mathbf{c}'_1, \ldots, \mathbf{c}'_{t+1-j}).$$

By Remark 2.1, Y' is $(j, t+1-j)$-separated if and only if $Y := Y' - \mathbf{c}'_{t+1-j}$ is. Hence it suffices to show that

$$Y = (\mathbf{a}_1, \ldots, \mathbf{a}_j; \mathbf{c}_1, \ldots, \mathbf{c}_{t-j}, \mathbf{0})$$

is $(j, t+1-j)$-separated.

Since the $t+1$ codewords of Y' are linearly independent, so are the t first codewords of Y. Now, consider

$$X := \{\mathbf{a}_1 + \mathbf{c}_1, \ldots, \mathbf{a}_1 + \mathbf{c}_{t-j}; \mathbf{a}_1, \ldots, \mathbf{a}_j\},$$

which is a set of linearly independent codewords from C, and hence all non-zero on some coordinate i. Since $\mathbf{a}_1 + \mathbf{c}_l$ is non-zero on coordinate i, $\mathbf{c}_l$ must be zero for all l. Hence Y, and consequently Y', is separated on coordinate i.

This completes the first step. In the case where $i \not\equiv j \pmod 2$, we get that t is even, and consequently the t first codewords of Y are linearly independent whenever any t words of Y' are. Therefore it is sufficient that any t codewords of Γ be linearly independent.

Finally, we consider the case where i and j are both even. We shall again show that Y' is separated. If all the $t+1$ words of Y' are linearly independent, then we are done by the first part of the proof. By assumption, we know that any $t-1$ words are linearly independent. This gives two cases to consider:

1. $\mathbf{c}'_{t+1-j}$ is the sum of the t first words, which are linearly independent.

2. $\mathbf{c}'_{t-j}$ is the sum of the $t-1$ first words and $\mathbf{c}'_{t+1-j}$ is independent of the others.

Let Y', Y, and X be defined as before. Consider the first case first. Any $t-1$ non-zero words of Y are linearly independent, while all the t non-zero words sum to $\mathbf{0}$. Hence, the only linear independence found between the elements of X is that

$$\mathbf{0} = \mathbf{b}_1 + \ldots + \mathbf{b}_{t-j} + \mathbf{a}_2 + \ldots + \mathbf{a}_j, \tag{5.1}$$

where $\mathbf{b}_i = \mathbf{c}_i + \mathbf{a}_1$. It follows that the $t-1$ first words of X intersect, since C is t-wise intersecting. Thus there is a position l, where $\mathbf{a}_i$ is 1 for $i = 1, \ldots, j-1$ and $\mathbf{c}_{i'}$ is zero for $i' = 1, \ldots, t-j$. Furthermore, $\mathbf{a}_j$ is one in position l by (5.1). Hence Y is separated.

In the second case, we get that the t non-zero words of Y are linearly independent. Thus the result follows like the first part of the proof. □

It is perhaps not obvious how these propositions may be used to construct non-linear separating codes with a reasonable rate. The remainder of the section is devoted to explaining this.

Lemma 4
Given an $[n, rm]$ linear, binary code C, we can extract a non-linear subcode Γ of size 2^r such that any $2m$ non-zero codewords are linearly independent.

Proof: Let C' be the $[2^r-1, 2^r-1-rm, 2m+1]$ BCH code. The columns of the parity check matrix of C' make a set Γ' of 2^r-1 vectors from $\mathsf{GF}(2)^{rm}$, such that no $2m$ of them are linearly independent. Now there is an isomorphism $\phi:\ \mathsf{GF}(2)^{rm} \to C$, so let $\Gamma = \phi(\Gamma') \cup \{\mathbf{0}\}$. □

Lemma 5
Given an $[n, rm+1]$ linear, binary code C, we can extract a non-linear subcode Γ of size 2^r+1 such that any $2m+1$ codewords are linearly independent.

Proof: Let C' be the $[2^r, 2^r-1-rm, 2m+2]$ extended BCH code. The columns of the parity check matrix of C' make a set Γ' of 2^r vectors from $\mathsf{GF}(2)^{rm+1}$, such that any $2m+1$ of them are linearly independent. Now there is an isomorphism $\phi:\ \mathsf{GF}(2)^{rm+1} \to C$, so let $\Gamma = \phi(\Gamma') \cup \{\mathbf{0}\}$. □

Problem 5.1 *Improve Lemmata 4 and 5.*

Theorem 10
Given an $[n, nR]$ t-wise intersecting binary (asymptotic) code, there is a construction of a non-linear (i,j)-SS Γ of rate $R/\lfloor t'/2 \rfloor$, where $j = t+1-i$, and $t' = t-1$ if i and j are even and $t' = t+1$ otherwise.

Proof: Set $j := t+1-i$, and let $\bar{t}(i,j)$ be as defined in Proposition 9. Observe that $\lfloor t'/2 \rfloor = \lfloor \bar{t}(i,j)/2 \rfloor$. By Lemma 4, we can construct an asymptotic code Γ with rate $R/\lfloor \bar{t}(i,j)/2 \rfloor = R/\lfloor t'/2 \rfloor$ where any $\bar{t}(i,j)$ codewords are linearly independent. Then Γ is (i,j)-separating by Proposition 9. □

(t,t')	SS rate
$(2,1)$	0.2075
$(3,1)$	0.03211
$(4,1)$	0.01164
$(5,1)$	0.003054
$(3,2)$	0.01164

(t,t')	SS rate
$(4,2)$	0.004580
$(5,2)$	0.001262
$(4,3)$	0.001262
$(5,3)$	0.0004041
$(5,4)$	0.0001765

(t,t)	SS rate
$(1,1)$	1
$(2,2)$	0.06422
$(3,3)$	0.003054
$(4,4)$	0.0005388
$(5,5)$	0.00006268

Table 5.1: Existence bounds on binary separating codes based on intersecting codes (Theorem 11).

Problem 5.2 *Is it possible to generate completely separating codes with good rates by a similar technique?*

5.3 Existence results

Using intersecting codes, we get the following existence bounds on separating codes. The numeric values for small t and u are shown in Table 5.1. Except for $(2,1)$- and $(2,2)$-SS, they are unfortunately not very good, as we will see in Chapter 6.

Theorem 11
For any i and any j, there exists asymptotically (i,j)-SS for any rate

$$R \leq \frac{1 - \frac{1}{t}\log(2^t - 1)}{\lfloor t'/2 \rfloor},$$

where $t = i + j - 1$ and $t' = t$ if i and j are both even and $t' = t + 1$ otherwise.

Proof: In [CZ94], it was shown that for sufficiently large n, and for any rate $R < 1 - \frac{1}{t}\log(2^t - 1)$, there are t-wise intersecting linear, binary $[n,k]$ codes of rate R. Applying this to Theorem 10, we get the result. □

5.4 Binary constructions

Several good (t,u)-separating codes may be constructed from intersecting codes and columns from the parity check matrices of BCH codes. In Table 5.2, we use a t-wise intersecting code from Proposition 10, and extract a non-linear subcode where any $\bar{t}$ words a linearly independent, using Lemma 4. This is concatenated with a Tsfasman code.

	Inters. code		Inner code		Outer code		rate
	t	$[n,k]$	$\bar{t}$	(n,M)	q	rate	
$(2,2)$	3	$[2^7-2,14]$	2	$(126,2^{14})$	2^{14}	123/508	0.02690
$(3,2)$	4	$[2^9-2,18]$	4	$(510,2^9)$	19^2	1/9	0.001851
$(3,3)$	5	$[2^{11}-2,22]$	6	$(2046,2^7)$	11^2	1/90	0.00003757
$(4,2)$	5	$[2^{11}-2,22]$	4	$(2046,2^{11})$	43^2	17/168	0.0005367
$(4,3)$	6	$[2^{13}-2,26]$	6	$(2^{13}-2,2^8)$	2^8	1/60	0.00001628
$(4,3)$	6	$[2^{15}-2,30]$	6	$(2^{15}-2,2^{10})$	2^{10}	19/372	0.00001559
$(4,4)$	7	$[2^{15}-2,30]$	6	$(2^{15}-2,2^{10})$	2^{10}	15/496	0.000009230
$(5,5)$	9	$[2^{25}-2,50]$	10	$(2^{25}-2,2^{10})$	2^{10}	6/775	$2.307 \cdot 10^{-9}$

Table 5.2: Constructions using punctured dual BCH codes (Prop. 10) as inner codes.

Note that for $(4,3)$-SS, two constructions are given. For the latter construction we use a 7-wise intersecting code in order to get a bigger alphabet for the outer code. This loses rate for the inner code, but gains for the outer code, and the two concatenated codes have roughly the same rate. For $(5,5)$-SS, the 9-wise intersecting dual BCH code is so small that the Tsfasman code cannot be constructed as outer code with positive rate. Instead we use a 13-wise intersecting code. Probably there are cleverer choices for inner codes than dual BCH codes.

Proposition 10 [CZ94]
The punctured dual of the 2-error-correcting BCH code with parameters $[2^{2t+1}-2, 4t+2, 2^{2t}-2^t-1]$, *is t-wise intersecting.*

Explicit constructions of infinite families of t-wise intersecting codes with non-zero rates where found om [CZ94]. These families give rise to separating codes.

Lemma 6 [CZ94]
Let C_1 be an $[n_1,k_1,d_1]_q$ code with $q = 2^{k_2}$ and minimum distance $d_1 > n_1(1-2^{1-t})$. Let C_2 be an $[n_2,k_2,d_2]$ binary t-wise intersecting code. Then the concatenation $C_1 \circ C_2$ is a binary t-wise intersecting $[n_1n_2,k_1k_2,d_1d_2]$ code.

Lemma 7 [CZ94]
There is a constructive infinite sequence of t-wise intersecting binary codes with rate arbitrarily close to

$$R_t = \left(2^{1-t} - \frac{1}{2^{2t+1}-1}\right)\frac{2t+1}{2^{2t}-1} = 2^{2-3t}(t+o(t)).$$

Proof: By concatenating geometric $[N,K,D]_q$ codes from Theorem 1 satisfying $D > N(1-2^{1-t})$ with $q = 2^{4t+2}$, and with a rate arbitrarily close to $2^{1-t} - 1/(\sqrt{q}-1)$, with the $[2^{2t+1}-2, 4t+2, 2^{2t}-2^t-1]$ code of Proposition 10, we obtain the result. □

Proposition 11
There is a constructive infinite sequence of binary $(j, t+1-j)$-separating codes of rate $2^{-3(t-1)}(1+o(1))$.

5.5 Upper bounds on intersecting codes

The upper bounds on intersecting codes are similar to those for separating codes as presented in Chapter 4. We include them here for reference.

Theorem 12
A t-wise intersecting code $C_t[n,k,d]$ gives rise by projection to a $(t-1)$-wise intersecting code $C_{t-1}[d,k-1]$.

Proof: Let $a \in C$ be a fixed element of minimum weight d. Denote by C_a the $[n,k-1]$ supplementary subspace of $\{\mathbf{0},a\}$ in C. Consider any $(t-1)$ independent codewords $\{b^1,\dots,b^{t-1}\}$ in C_a. Then $\{a,b^1,\dots,b^{t-1}\}$ is full rank, hence these t codewords of C intersect (on the support of a). Thus C/a, the projection of C_a on the support of a is a $(t-1)$-wise intersecting $[d,k-1]$ code. □

To get an upper bound on the dimension of such codes in the binary case, we use recursively the best known upper bound on error correcting codes, namely the McEliece et al. bound (see Theorem 6).

For $t=3$, we get the following sequence of codes:

$$C_3[n,k,d], \quad C_2[d,k-1,d'], \quad C_1[d',k-2],$$

where C_i is i-wise intersecting, and has write rate R_i.

From C_1, we have that $k-2 \le d'$, which implies that

$$R_2 = (k-1)/d \le (d'-1)/d \le d'/d.$$

By the McEliece bound, this implies $R_2 \le 0.28$. Finally we have

$$R_1 = \frac{k}{n} \le \frac{0.28d+1}{n} \le 0.108,$$

where the final bound follows by applying again the McEliece bound. The following corollary arise from the same technique and some other values for t.

Corollary 5
The asymptotic rate of the largest t-wise intersecting binary code is at most R_t, with $R_2 \approx 0.28, R_3 \approx 0.108, R_4 \approx 0.046, R_5 \approx 0.021, R_6 \approx 0.0099$.

Note that the McEliece bound is only valid asymptotically. In particular, the $[126, 14]$ 3-wise intersecting code from Proposition 10 has rate $1/9 > R_3$.

Chapter 6

Existence bounds

Random coding is a standard technique for proving lower bounds on codes, for separating codes as well as error-correcting codes. In this chapter, we spell out a general framework of this technique, with a few variations.

6.1 Random coding bound

Let C be a random (n, M)-code (uniform distribution) and compute the expected number $\mathcal{E}$ of (t, u)-configurations (T, U) which are not separated. Whenever $\mathcal{E} \leq M/2$ there is at least one code C_0 with at most $M/2$ bad configurations, and if we remove one word from each bad configuration, we get an $(n, M/2)$ code with the (t, u)-separating property.

The probability that a coordinate i separate U and T is independent of the choice of i by the randomness assumption; denote it by $p(q, t, u)$. The probability that a given (T, U) is not separated is

$$P_{q,t,u,n} = (1 - p(q, t, u))^n, \tag{6.1}$$

which implies

$$\mathcal{E} = \binom{M}{t+u}\binom{t+u}{t} P_{q.t,u,n}. \tag{6.2}$$

Writing $M = q^{Rn}$ and letting n go to infinity, we get that infinite sequences of (t, u)-separating codes exist for all rates R such that $\log_q \mathcal{E} < Rn$, i.e. such that

$$(t+u)R + \frac{1}{n}\log_q P_{q,t,u,n} < R.$$

Making use of (6.1), we get the following proposition.

Proposition 12
Infinite sequences of (t,u)-separating codes exist for all rates R such that

$$R < \frac{1}{t+u-1} \log_q (1 - p(q,t,u))^{-1}.$$

We now apply the previous proposition to specific values of q,t,u.

Theorem 13 (Binary lower bound)
There is an infinite family of binary (t,u)-SS with rate

$$R_2(t,u) \geq \max_{0 \leq \wp \leq 1} \frac{1}{t+u-1} \log_2 \left(1 - \wp^t \cdot (1-\wp)^u - \wp^u \cdot (1-\wp)^t\right)^{-1}.$$

Proof: Let $\wp$ denote the probability of choosing a 1 in a given position in a given word. We get that

$$p(2,t,u) = \wp^t \cdot (1-\wp)^u + \wp^u \cdot (1-\wp)^t.$$

Thus the theorem follows from Proposition 12. □

Problem 6.1 *The analogous bound for superimposed codes is maximised for $\wp = t/(t+u)$. Find analytically the value of $\wp$ which maximises the bound in Theorem 13.*

For $(2,1)$- and $(2,2)$-SS, this gives the well-known bounds [Sag94], which also coïncide with the bounds from intersecting codes in Section 5.3. Numerical values are given in Table 6.1.

Theorem 14 (Lower bound for large alphabets)
If $q > tu$, there exists an asymptotic, q-ary (t,u)-SS with rate $R \approx (t+u-1)^{-1}(1 - \log_q tu)$.

Proof: We prove that such codes exist with uniform distribution in each coordinate position. Since $q > tu$, we get that

$$p(q,t,u) \geq ((q-t)/q)^u \geq 1 - tu/q.$$

Now the theorem follows directly from Proposition 12. □

Letting q tend to infinity, we also get the following corollary.

Corollary 6
For sufficiently large q, there exists an asymptotic, q-ary (t,u)-SS with rate $R \approx (t+u-1)^{-1}$.

	$\wp = 1/2$	Theorem 13		Theorem 15	
(t,t')	R	R	$\wp$	R	q
(2,1)	0.2075	0.2075	0.5000000	0.1491	3
(3,1)	0.06422	0.06422	0.5000667	0.06928	5
(4,1)	0.02328	0.03138	0.7886795	0.03999	6
(5,1)	0.009161	0.02004	0.8322462	0.02595	8
(2,2)	0.06422	0.06422	0.5000000	0.04029	2
(3,2)	0.02328	0.02328	0.5000000	0.01584	2
(4,2)	0.009161	0.009160	0.5000000	0.007402	2
(5,2)	0.003787	0.003991	0.6666755	0.003828	2
(3,3)	0.009161	0.009161	0.5000000	0.005707	2
(4,3)	0.003787	0.003787	0.5000000	0.002456	2
(5,3)	0.001616	0.001616	0.5000000	0.001204	2
(4,4)	0.001616	0.001616	0.5000000	0.0009489	2
(5,4)	0.0007058	0.0007058	0.5000000	0.0004229	2
(5,5)	0.0003134	0.0003134	0.5000000	0.0001686	2

Table 6.1: Numerical values of the lower bounds given by Theorems 13 and 15, with optimal choices for q and $\wp$. We also give the lower bounds obtained by random coding with symbol probability $\wp = 0.5$.

The best known upper bound on (t,u)-SS for large q is $R \leq 1/t$, which is the bound on $(t,1)$-SS. Observe that for moderate u, this upper bound is rather close to the upper bound proved above.

Conjecture 1
For q sufficiently large, the best possible asymptotic rate for (t,u)-SS is $R = (t+u-1)^{-1}$.

This conjecture has been proved for $(2,2)$-SS (see [Sag94]) as well as for $(t,1)$-SS as we saw in Chapter 3. Blackburn [Bla03a] also asked how the rate behaves when the length n is fixed and the alphabet size q tends to infinity. For $(t,1)$-SS this was answered in [Bla03b].

6.2 Random constant-weight coding bound

In this section we consider binary separating codes with constant weight. In some cases, we can prove that such codes exist with rates above the bound from Theorem 13. This technique was established for superimposed codes in [AZ88].

Let $q \geq 2$ be an arbitrary integer. The constant-weight code is obtained by concatenating a random $(w,M)_q$ code with an $(q,q,2)_2$ inner code, where all words have weight 1. Clearly this gives an $(n = qw, M)_2$ code where all the words have weight w. The random outer code is built by choosing for each coordinate in each codeword an element from Z_q with uniform probability.

The bits corresponding to one position in the outer code will be referred to as a *block*. Thus the code has length w blocks or n bits. The following argument is analog to that of the previous section, working on blocks rather than on individual coordinate positions.

Let T and U be disjoint sets of codewords of sizes t and u respectively. The probability that T and U be separated on block i is independent of i, and is denoted $p(q,t,u)$. The probability that T and U are not separated at all is

$$P_{q,t,u,w} = (1 - p(q,t,u))^w. \tag{6.3}$$

The expected number of non-separated pairs is $\mathcal{E}$ as given in (6.2), and letting n go to infinity, we get that (t,u)-SS exist for all rates R such that $\log_2 \mathcal{E} < Rqw$, i.e. such that

$$R < -\frac{1}{t+u-1}\frac{1}{q}\log_2(1 - p(q,t,u)). \tag{6.4}$$

It remains to calculate $p(q,t,u)$.

Write the elements of T and U as $(\mathbf{x}_1,\ldots,\mathbf{x}_t;\mathbf{y}_1,\ldots,\mathbf{y}_u)$. Since a codeword has one and only one 1-bit in each block, each block has at most one column of the form $\mathbf{a}_1 = (1,\dots,1;0,\dots,0)$ and at most one of the form $\mathbf{a}_2 = (0,\dots,0;1,\dots,1)$ in block i.

The probability of having a column of form $\mathbf{a}_1$ in block i is

$$P_1 = \left(\frac{1}{q}\right)^{t-1}\left(1-\frac{1}{q}\right)^{u}, \tag{6.5}$$

because the $\mathbf{x}_1$ can be chosen freely, while $\mathbf{x}_2,\dots,\mathbf{x}_t$ must have the same symbol in block i of the outer code. All the vectors $\mathbf{y}$ must have a different symbol in the outer code. Likewise the probability of having a column $\mathbf{a}_2$ is

$$P_2 = \left(\frac{1}{q}\right)^{u-1}\left(1-\frac{1}{q}\right)^{t}. \tag{6.6}$$

The probability of having both column types $\mathbf{a}_1$ and $\mathbf{a}_2$ is

$$P_{1,2} = \left(1-\frac{1}{q}\right)\left(\frac{1}{q}\right)^{t+u-2}. \tag{6.7}$$

By common inclusion-exclusion, we get $p(q,t,u) = P_1 + P_2 - P_{1,2}$.

Theorem 15 (Binary lower constant-weight bound)
There an infinite family of binary (t,u)-SS with rate

$$R_2(t,u) \geq \max_{q=2,3,\dots} \frac{-1}{q(t+u-1)} \log_2 P^*(q,t,u),$$

where

$$P^*(q,t,u) = \left[1-\left(\frac{1}{q}\right)^{t-1}\left(1-\frac{1}{q}\right)^{u}-\left(\frac{1}{q}\right)^{u-1}\left(1-\frac{1}{q}\right)^{t}+\left(1-\frac{1}{q}\right)\left(\frac{1}{q}\right)^{t+u-2}\right].$$

Numerical values are given in Table 6.1. Note that constant weight codes only improve the bounds for $(t,1)$-SS for $t > 2$. Furthermore, these bounds match exactly the bounds on $(t,1)$-superimposed codes as given in [DVMT02].

Problem 6.2 *For $(t,1)$-separating code, we have constructive lower bounds on the rate for a given separating weight τ, and [DRR89] gives an existence bound for $(t,1)$-superimposed codes with a given superimposed distance. Is it possible to get stronger results for $(t,1)$-SS with a guaranteed separating weight by some form of random coding?*

Problem 6.3 *Develop a lower bound on the rate of (t,u)-SS, $t \geq u \geq 2$, for a guaranteed separating weight τ.*

Problem 6.4 *For $(t, 1)$-superimposed codes, better rates can be obtained by considering random constant-weight codes. That result appeared in [DRR89], and numerical results were presented in [DMR00]. Give an analogous proof for separating codes.*

Problem 6.5 *In [DVMT02], the authors suggest that results from [DRR89] can be extended for (t,u)-superimposed codes with $u > 1$. Can this be done for (t,u)-SS as well?*

6.3 Lower bound on superimposed codes

The bounds presented in this chapter are very similar to the ones given for superimposed codes in [DVMT02, Section 3.5]. To show this analogue, we include their result as well.

Theorem 16
For any $t \geq u \geq 1$, the best asymptotic rate of a (t,u)-superimposed code is at least

$$R \geq \frac{\max E_1(t,u), E_2(t,u)}{t+u-1}, \tag{6.8}$$

where

$$E_1(t,u) = -\log_2\left(1 - \frac{t^t u^u}{(t+u)^{t+u}}\right), \tag{6.9}$$

$$E_2(t,u) = \max_{q=2,3,\dots} -\log_2\left[1 - \left(\frac{1}{q}\right)^{t-1}\left(1-\frac{1}{q}\right)^u\right]. \tag{6.10}$$

The bound given by E_1 is correspond to Theorem 13, where $p(2,t,u) = \wp^t(1-\wp)^u$ contains one term instead of two, as only one column type gives the superimposition property. The maximising value of $\wp$ is $t/(t+u)$.

The bound given by E_2 correspond to Theorem 15, where $p(q,t,u) = P_2$, again because only the column type $\mathbf{a}_2$ gives superimposition.

Chapter 7

On $(2,1)$- and $(2,2)$-separation

The two simplest cases $(2,1)$- and $(2,2)$-separation are the ones most studied in the literature. It has been found that Proposition 1 can be considerably strengthened in these cases. Except for the construction of an asymptotic $(2,1)$-SS with rate 0.1845, all the results in this chapter have appeared elsewhere, and most of them are even well-known classics. We include them for reference.

Theorem 17
If Γ is a code with minimum distance d_1 and maximum distance m_1, then $2\theta_{2,1} \geq 2d_1 - m_1$.

Proof: Let $(\mathbf{c};\mathbf{a},\mathbf{b})$ be a $(2,1)$-configuration. Letting the three words be rows of a matrix, we have essentially four types of columns: Type 0 where all the elements are equal, Type I where **a** or **b** differs from the two others, Type A where **c** differs from the two others, and Type B with three different elements. Let v_i denote the number of elements of Type i.

Consider the sum

$$\Sigma := w(\mathbf{c}-\mathbf{a}) + w(\mathbf{c}-\mathbf{b}) \geq 2d.$$

Observe that

$$\Sigma = 2(v_\mathrm{A} + v_\mathrm{B}) + v_\mathrm{I}.$$

Clearly we have

$$\theta(\mathbf{c};\mathbf{a},\mathbf{b}) = v_\mathrm{A} + v_\mathrm{B},$$

and

$$w(\mathbf{a}-\mathbf{b}) = v_\mathrm{B} + v_\mathrm{I},$$

so $v_\mathrm{I} \leq m_1$. It follows that

$$2\theta(\mathbf{c};\mathbf{a},\mathbf{b}) \geq 2d_1 - m_1.$$

□

For $(2,2)$-SS, the situation is not as clear as it is for $(2,1)$-SS. We get a similar result for the binary case only (Theorem 18). In the non-binary case we get only a sufficient condition for $\theta_{2,2} > 0$ (Theorem 19).

Theorem 18
Let Γ be a binary code with minimum distance d_1 and maximum distance m_1. Then $4\theta_{2,2} \geq 4d_1 - 2m_1 - n$. If Γ is linear, then $4\theta_{2,2} \geq 4d_1 - 3m_1$.

This result is a classic one which dates at least from [Sag75]. A proof can be found in [KS02], where they also show and use the fact that if the non-linear code Γ is contained in a linear code C with maximum distance m'_1, then $4\theta_{2,2} \geq 4d_1 - 2m_1 - m'_1$.

In the non-binary case, we have not managed to find a bound on $\theta_{2,2}$, but we have a sufficient condition for $(2,2)$-separation. The following theorem appeared in [CES02] and the proof will be given in the following section.

Theorem 19
If a code satisfies $4d_1 > 2m_1 + n$, or if $4d_1 > 3m_1$ and it is linear, then it is $(2,2)$-separating.

7.1 On $(2,2)$-SS

Let Γ be an (n,M) code with minimum weight d_1 and maximum weight m_1. Let $(\{\mathbf{c}',\mathbf{c}\},\{\mathbf{a},\mathbf{b}\})$ be a $(2,2)$-configuration which is not separated. We shall deduce some conditions on d_1 and m_1 which are necessary if $(\{\mathbf{c}',\mathbf{c}\},\{\mathbf{a},\mathbf{b}\})$ not be separated. By inverting this conditions, we get sufficient conditions for Γ being separating.

By Remark 2.1, we can assume that $\mathbf{c}' = \mathbf{0}$ and $\mathbf{c} = (1,\dots,1,0,\dots,0)$. We write

$$\begin{aligned}\mathbf{c} &= (c_1, c_2, \dots, c_n),\\ \mathbf{a} &= (a_1, a_2, \dots, a_n),\\ \mathbf{b} &= (b_1, b_2, \dots, b_n).\end{aligned}$$

Let r be such that $c_i = 1$ for $i \leq r$ and $c_i = 0$ for $i > r$.

We consider the sum

$$\begin{aligned}\Sigma &:= d(\mathbf{0},\mathbf{a}) + d(\mathbf{0},\mathbf{b}) + d(\mathbf{c},\mathbf{a}) + d(\mathbf{c},\mathbf{b})\\ &= w(\mathbf{a}) + w(\mathbf{b}) + w(\mathbf{a}-\mathbf{c}) + w(\mathbf{b}-\mathbf{c}).\end{aligned}$$

We have trivially that

$$4d_1 \leq \Sigma \leq 4m_1. \tag{7.1}$$

Consider now the matrix with rows $\mathbf{0},\mathbf{c},\mathbf{a},\mathbf{b}$. Let $\mathbf{x}_i$ be the i-th column in this matrix. We have four main types of columns:

$$\begin{aligned}
\text{Type 0}: &\quad \mathbf{x}_i = (0,0,0,0), && \\
\text{Type I}: &\quad \mathbf{x}_i \in \{(0,0,0,\alpha),(0,0,\alpha,0)\}, && \alpha \neq 0, \\
\text{Type IIa}: &\quad \mathbf{x}_i \in \{(0,1,0,0),(0,1,1,1)\}, && \\
\text{Type IIb}: &\quad \mathbf{x}_i \in \{(0,1,0,1),(0,1,1,0)\}, && \\
\text{Type III}: &\quad \mathbf{x}_i \in \{(0,1,0,\beta),(0,1,\beta,0),(0,1,1,\beta),(0,1,\beta,1)\}, && \beta \notin \{0,1\}.
\end{aligned}$$

We have now that

$$\Sigma = \sum_{i=1}^{n} \sigma(\mathbf{x}_i), \tag{7.2}$$

where $\sigma(\mathbf{x}_i)$ is 0 for Type 0, 2 for Types I and II, and 3 for Type III. Let v_{X} denote the number of columns of Type X. Then we get

$$n = v_0 + v_{\mathrm{I}} + v_{\mathrm{II}} + v_{\mathrm{III}}, \tag{7.3}$$

$$\Sigma = 2v_{\mathrm{I}} + 2v_{\mathrm{II}} + 3v_{\mathrm{III}}. \tag{7.4}$$

Proposition 13
If $(\mathbf{0},\mathbf{c};\mathbf{a},\mathbf{b})$ *is not* $(2,2)$*-separated, then*

$$\Sigma = w(\mathbf{c}) + w(\mathbf{a}-\mathbf{b}) + w(\mathbf{a}+\mathbf{b}-\mathbf{c}).$$

Proof: We have trivially that

$$n - w(\mathbf{c}) = v_0 + v_{\mathrm{I}}. \tag{7.5}$$

Define two words

$$\begin{aligned}
\mathbf{y} &= (y_1,y_2,\ldots,y_n) := \mathbf{a}+\mathbf{b}-\mathbf{c}, \\
\mathbf{z} &= (z_1,z_2,\ldots,z_n) := \mathbf{a}-\mathbf{b}.
\end{aligned}$$

We have that

$$\begin{aligned}
\mathbf{x}_i \text{ of Type 0} &\quad\Rightarrow y_i = 0 \quad\wedge\quad z_i = 0, \\
\mathbf{x}_i \text{ of Type I} &\quad\Rightarrow y_i = 1 \quad\wedge\quad z_i = \pm 1, \\
\mathbf{x}_i \text{ of Type IIa} &\quad\Rightarrow y_i = \pm 1 \quad\wedge\quad z_i = 0, \\
\mathbf{x}_i \text{ of Type IIb} &\quad\Rightarrow y_i = 0 \quad\wedge\quad z_i = \pm 1, \\
\mathbf{x}_i \text{ of Type III} &\quad\Rightarrow y_i \in \{\beta,\beta-1\} = \{\alpha \neq 0\} \\
&\qquad \wedge z_i \in \{\pm(\beta-1),\pm\beta\} = \{\alpha \neq 0\}.
\end{aligned}$$

This gives

$$n - w(\mathbf{a}+\mathbf{b}-\mathbf{c}) = n - w(\mathbf{y}) = v_0 + v_{\mathrm{IIb}},$$
$$n - w(\mathbf{a}-\mathbf{b}) = n - w(\mathbf{z}) = v_0 + v_{\mathrm{IIa}}.$$

By adding together the two equations above as well as (7.5), we get

$$3n - (w(\mathbf{c}) + w(\mathbf{a}-\mathbf{b}) + w(\mathbf{a}+\mathbf{b}-\mathbf{c})) = 3v_0 + v_{\mathrm{IIa}} + v_{\mathrm{IIb}} + v_{\mathrm{I}}.$$

From (7.4) and (7.3) we get that

$$\Sigma = 3n - (3v_0 + v_{\mathrm{IIa}} + v_{\mathrm{IIb}} + v_{\mathrm{I}}) = w(\mathbf{c}) + w(\mathbf{a}-\mathbf{b}) + w(\mathbf{a}+\mathbf{b}-\mathbf{c}), \tag{7.6}$$

as required. □

We observe that $d(\mathbf{a},\mathbf{b}) = w(\mathbf{a}-\mathbf{b})$ and $d(\mathbf{0},\mathbf{c}) = w(\mathbf{c})$ are distances in the code; hence they are bounded by m_1. If C is linear, $w(\mathbf{a}+\mathbf{b}-\mathbf{c})$ is also a distance in the code, and thus bounded by m_1. If C is non-linear, we still have $w(\mathbf{a}+\mathbf{b}-\mathbf{c}) \leq n$. This gives Theorem 19.

Example 7.1 *From the proposition we get that if* $(\mathbf{0},\mathbf{c};\mathbf{a},\mathbf{b})$ *is a binary* $(2,2)$*-NSC and* $4d_1 = 3m_1$*, then*

$$w(\mathbf{c}) = w(\mathbf{a}-\mathbf{b}) = w(\mathbf{a}+\mathbf{b}-\mathbf{c}) = m_1 = 4l,$$
$$w(\mathbf{a}) = w(\mathbf{b}) = w(\mathbf{a}-\mathbf{c}) = w(\mathbf{b}-\mathbf{c}) = d_1 = 3l.$$

It turns out that the only possible $(2,2)$*-NSC is the following, or replications thereof:*

$$\begin{bmatrix} \mathbf{0} \\ \mathbf{c} \\ \mathbf{a} \\ \mathbf{b} \end{bmatrix} = \begin{bmatrix} 000000 \\ 111100 \\ 110010 \\ 101001 \end{bmatrix}.$$

Note that the linear code $\langle \mathbf{a},\mathbf{b},\mathbf{c} \rangle$ *has also* $d_1 = 3$ *and* $m_1 = 4$.

7.2 Asymptotic results in binary

In Table 7.1, we present up to date bounds on $(2,1)$- and $(2,2)$-SS. The construction of non-linear $(2,1)$-SS is new, and thus is presented in the following section.

Bound	$(2,1)$-SS	$(2,2)$-SS
Linear construction	0.156[1]	0.02622[4]
Linear existence	0.2075[1]	0.0642[Sag82]
Non-linear construction	0.1845[2]	—
Non-linear existence	0.2075[3]	—
Linear upper bound	0.28 [1]	0.108[CEL01]
Non-linear upper bound	0.5[3]	0.2835 [Sag94]

[1] Bounds from intersecting codes [CZ94]. These bounds are also stated in [Sag94], with the possible exception of the construction.
[2] Kerdock-Tsfasman construction (this section).
[3] [Kör95]. Theorem 3 provides an alternative proof for the upper bound.
[4] BCH/intersecting construction.

Table 7.1: Bounds on rates for infinite families of binary $(2,1)$-SS and $(2,2)$-SS.

Property	$\theta_{t,u} \geq$	min. m	n	$\log M$
$(2,1)$-SS	$2^{m-2} - 3 \cdot 2^{m/2-2}$	4	15	7
$(2,2)$-SS	$2^{m-4} - 3 \cdot 2^{m/2-2}$	8	255	15

Table 7.2: Kerdock codes and separating properties.

7.2.1 Kerdock constructions

In [KS02], it was pointed out that shortened Kerdock codes have some nice separating properties. Here we shall combine this discovery with the Tsfasman codes to break some asymptotic records.

The Kerdock codes [Ker72], which are defined for $m \geq 4$ and m even, are non-linear, binary codes with parameters $(2^m, 2^{2m}, 2^{m-1} - 2^{m/2-1})$. The Kerdock codes have only four non-zero weights, $\{2^{m-1} - 2^{m/2-1}, 2^{m-1}, 2^{m-1} + 2^{m/2-1}, 2^m\}$. By shortening the Kerdock codes on one position, we get rid of the all-one word, and obtain a class of three-weight codes $K'(m)$, where

$$
\begin{aligned}
n &= 2^m - 1, \\
\log M &= 2m - 1, \\
d_1 &= 2^{m-1} - 2^{m/2-1}, \\
m_1 &= 2^{m-1} + 2^{m/2-1}.
\end{aligned}
$$

Krasnopev and Sagalovich showed that for $m \geq 4$, $K'(m)$ is a $(2,1)$-SS, and for $m \geq 8$, it is a $(2,2)$-SS. The fact that $K'(m)$ for $m \geq 4$ is $(2,1)$-separating follows directly from Theorem 17. Proving any lower bound on $\theta_{2,2}$ requires the following two lemmata.

Lemma 8
The one-shortened Kerdock code $K'(m)$ is a subcode of the one-shortened, second-order Reed-Muller code, which is linear.

This lemma follows from the fact that $K(m)$ is a subcode of the second-order Reed-Muller code.

Lemma 9
The one-shortened, second-order Reed-Muller code has maximum distance $m'_1 = 3 \cdot 2^{m-2}$.

Considering the expression for Σ in (7.6), we see that $K'(m)$ is $(2,2)$-separating. The two first weights are distances in $K'(m)$ and bounded by m_1. The third weight is a weight in the one-shortened, second-order Reed-Muller code, and thus bounded by m'_1. Thus $K'(m)$ is a $(2,2)$-SS whenever $4d > 2m_1 + m'_1$, which holds for $m \geq 8$ as claimed. The details on these codes are shown in Table 7.2.

The $(2,1)$-SS obtained is a good one, and if we concatenate it with a Tsfasman code of rate $1/2 - 1/10$ and minimum distance $\delta = 1/2$ over $\mathsf{GF}(11^2)$, we get an asymptotic class of $(2,1)$-SS with rate 0.1845 which is a new record.

Unfortunately, it does not appear to be possible to get any stronger separation properties in this way, and the $(2,2)$-SS is not a record breaker.

If we could use the AG codes from [Xin02] (see the following theorem) as outer codes, we would get a $(2,1)$-SS with rate 0.2033, but Xing's theorem is non-constructive.

Theorem 20 (Xing)
Suppose that $q = p^{2r}$ with p prime, and that s is an integer such that $2 \leq t \leq \sqrt{q}-1$. Then there is an asymptotic family of $(t,1)$-separating codes with rate

$$R = \frac{1}{t} - \frac{1}{\sqrt{q}-1} + \frac{1-2\log_q t}{t(\sqrt{q}-1)}.$$

Chapter 8

Asymptotic Results

In Table 8.1, we present the known upper and lower bounds for (t,u)-SS with certain t and u. Most of the bounds have been presented in previous chapters.

The best constructions of $(t,1)$-SS originates from [CE00a], where finite frame-proof codes designed by Stinson and Wei (see Lemma 10 below) are concatenated with Tsfasman codes. We can improve this construction significantly by using a larger, q-ary alphabet for the outer code, where q is not a power of 2. These new improved constructions are presented in Table 8.2.

Lemma 10 [SW98]
For any prime power v, there is a constructible, binary $(\lfloor v/2 \rfloor, 1)$-SS with parameters (v^2+1, v^3+v).

Problem 8.1 *Very good constructions of superimposed codes are presented in [DMR00]. Can those techniques be used to obtain better inner codes and thus improve the present asymptotic constructions?*

	Lower bounds		Upper bounds
(t,t')	Constructive	Non-constructive	
$(2,1)$	0.1845[1]	0.2075[1]	0.5[1,6]
$(3,1)$	0.04428[2]	0.06928[9]	0.3333[6]
$(4,1)$	0.02453[2]	0.03999[9]	0.25[6]
$(5,1)$	0.01375[2]	0.02595[9]	0.2[6]
$(2,2)$	0.02690[4]	0.06422[3,8]	0.2835[7]
$(3,2)$	0.001851[4]	0.02328[8]	0.1202[7]
$(4,2)$	0.0005367[4]	0.009161[8]	0.07994[7]
$(3,3)$	0.00003757[4]	0.009161[8]	0.0658[5]
$(4,3)$	0.00001628[4]	0.003787[8]	0.02951[7]
$(4,4)$	0.000009230[4]	0.001616[8]	0.01630[7]
$(5,5)$	$2.307 \cdot 10^{-9}$[4]	0.0003134[8]	0.004037[7]

[1] See Section 7.2.
[2] Stinson-Wei-Tsfasman constructions. See Table 8.2.
[3] Theorem 11.
[4] Intersection-Tsfasman codes from Section 5.4.
[5] Statement from [CGL01], no proof is found. The bound from Chapter 4 is slightly inferior.
[6] Theorem 3.
[7] Chapter 4.
[8] Theorem 13.
[9] Theorem 15.

Table 8.1: Bounds on rates for infinite families of binary codes with various separating properties.

	Inner code			Outer code		rate
	v	(n,M)	rate	field	rate	
$(3,1)$-SS	7	$(50,350)$	0.1635	$\mathsf{GF}(17^2)$	13/48	0.04428
$(4,1)$-SS	9	$(82,738)$	0.1160	$\mathsf{GF}(27^2)$	11/52	0.02453
$(5,1)$-SS	11	$(122,1342)$	10/122	$\mathsf{GF}(2^{10})$	26/155	0.01375

Table 8.2: Stinson-Wei-Tsfasman constructions.

Bibliography

[Aal90] Matti Aaltonen. A new upper bound on nonbinary block codes. *Discrete Math.*, 83(2-3):139–160, 1990.

[Alo86] N. Alon. Explicit construction of exponential sized families of k-independent sets. *Discrete Math.*, 58(2):191–193, 1986.

[AZ88] Nguyen Quang A and T. Zeisel. Bounds on constant weight binary superimposed codes. *Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform.*, 17(4):223–230, 1988.

[BBK01a] A. Barg, G. R. Blakley, and G. Kabatiansky. Good digital fingerprinting codes. Technical report, DIMACS, 2001.

[BBK01b] A. Barg, G. R. Blakley, and G. Kabatiansky. Good digital fingerprinting codes. In *Proc. IEEE Intern. Symp. Inform. Theory*, 2001.

[BCE+01] A. Barg, G. Cohen, S. Encheva, G. Kabatiansky, and G. Zémor. A hypergraph approach to the identifying parent property. *SIAM J. Disc. Math.*, 14(3):423–431, 2001.

[Bla03a] Simon R. Blackburn. Combinatorial schemes for protecting digital content. 2003. To appear.

[Bla03b] Simon R. Blackburn. Frameproof codes. *SIAM J. Discrete Math.*, 2003. To appear.

[BR80] Bella Bose and T. R. N. Rao. Separating and completely separating systems and linear codes. *IEEE Trans. Comput.*, 29(7):665–668, 1980.

[BS98] Dan Boneh and James Shaw. Collusion-secure fingerprinting for digital data. *IEEE Trans. Inform. Theory*, 44(5):1897–1905, 1998. Presented in part 1995, see Springer LNCS.

[BW98] Simon R. Blackburn and Peter R. Wild. Optimal linear perfect hash families. *Journal of Combinatorial Theory. Series A*, 83:233–250, 1998.

[CE00a] Gérard D. Cohen and Sylvia B. Encheva. Efficient constructions of frameproof codes. *Electronic Letters*, 36(22), 2000.

[CE00b] Gérard D. Cohen and Sylvia B. Encheva. Intersecting codes and partially identifying codes. Technical report, Ecole Nationale Supérieure des Télécommunications, September 2000.

[CE01] Gérard D. Cohen and Sylvia B. Encheva. Identifying codes for copyright protection. Technical report, Ecole Nationale Supérieure des Télécommunications, 2001.

[CEL01] Gérard D. Cohen, Sylvia B. Encheva, and Simon Litsyn. Intersecting codes and partially identifying codes. In Daniel Augot, editor, *Workshop on Coding and Cryptography*, January 2001.

[CELS01] Gérard D. Cohen, Sylvia B. Encheva, Simon Litsyn, and Hans Georg Schaathun. Intersecting codes and separating codes. *Discrete Applied Mathematics*, 2001. To appear.

[CES01] Gérard D. Cohen, Sylvia B. Encheva, and Hans Georg Schaathun. On separating codes. Technical report, Ecole Nationale Supérieure des Télécommunications, 2001.

[CES02] Gérard D. Cohen, Sylvia B. Encheva, and Hans Georg Schaathun. More on $(2, 2)$-separating codes. *IEEE Trans. Inform. Theory*, 48(9):2606–2609, September 2002.

[CFN94] B. Chor, A. Fiat, and M. Naor. Tracing traitors. In *Advances in Cryptology - CRYPTO '94*, volume 839 of *Springer Lecture Notes in Computer Science*, pages 257–270. Springer-Verlag, 1994.

[CGL01] Fan Chung, Ronald Graham, and Tom Leighton. Guessing secrets. *Electron. J. Combin.*, 8, 2001.

[Cha90] I. M. Chakravarti. Families of codes with few distinct weights from singular and non-singular hermitian varieties and quadrics in projective geometries and hadamard difference sets and designs associated with two-weight codes. *Coding theory and design theory, Part 1*, pages 35–50, 1990.

[CS03a] Gérard D. Cohen and Hans Georg Schaathun. Presented at CCC'03 in Yellow Mountain, China., 2003.

[CS03b] Gérard D. Cohen and Hans Georg Schaathun. New upper bounds on separating codes. In *2003 International Conference on Telecommunications*, February 2003.

[CZ94] Gérard Cohen and Gilles Zémor. Intersecting codes and independent families. *IEEE Trans. Inform. Theory*, 40:1872–1881, 1994.

[DMR00] Arkadii G. D′yachkov, Anthony J. Macula, Jr., and Vyacheslav V. Rykov. New constructions of superimposed codes. *IEEE Trans. Inform. Theory*, 46(1):284–290, 2000.

[DR83] A. G. D′yachkov and V. V. Rykov. A survey of superimposed code theory. *Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform.*, 12(4):229–242, 1983. English translation from Russian.

[DRR89] A. G. D′yachkov, V. V. Rykov, and A. M. Rashad. Superimposed distance codes. *Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform.*, 18(4):237–250, 1989.

[DS98] Stefan Dodunekov and Juriaan Simonis. Codes and projective multisets. *Electron. J. Combin.*, 5(1), 1998. Research Paper 37.

[DVMT02] A. G. D′yachkov, P. Vilenkin, A. Macula, and D. Torney. Families of finite sets in which no intersection of ℓ sets is covered by the union of s others. *J. Combin. Theory*, 99:195–208, 2002.

[EC99] Sylvia B. Encheva and Gérard D. Cohen. Constructions of intersecting codes. *IEEE Trans. Inform. Theory*, 45(4):1234–1237, 1999.

[FGU69] A. D. Friedman, R. L. Graham, and J. D. Ullman. Universal single transition time asynchronous state assignments. *IEEE Trans. Comput.*, 18:541–547, 1969.

[GSW00] J. Garay, J. Staddon, and A. Wool. Long-lived broadcast encryption. In *Crypto 2000*, volume 1880 of *Springer Lecture Notes in Computer Science*, pages 333–352, 2000.

[HK95] Tor Helleseth and P. Vijay Kumar. The weight hierarchy of the Kasami codes. *Discrete Math.*, 145(1-3):133–143, 1995.

[HKM77] Tor Helleseth, Torleiv Kløve, and Johannes Mykkeltveit. The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l - 1)/n)$. *Discrete Math.*, 18:179–211, 1977.

[HKY92] Tor Helleseth, Torleiv Kløve, and Øyvind Ytrehus. Generalized Hamming weights of linear codes. *IEEE Trans. Inform. Theory*, 38(3):1133–1140, 1992.

[HvLLT98] Henk D. L. Hollmann, Jack H. van Lint, Jean-Paul Linnartz, and Ludo M. G. M. Tolhuizen. On codes with the identifiable parent property. *J. Combin. Theory Ser. A*, 82(2):121–133, 1998.

[Ker72] A. M. Kerdock. A class of low-rate nonlinear binary codes. *Information and Control*, 20:182–187; ibid. **21 (1972), 395**, 1972.

[KLO03] Hyun Kwang Kim, Vladimir Lebedev, and Dong Yeol Oh. Some new results on (w,r) superimposed codes. Submitted to WCC'03., 2003.

[KM88] J. Körner and K. Marton. New bounds for perfect hashing via information theory. *European Journal of Combinatorics*, 9:523–530, 1988.

[Kör95] János Körner. On the extremal combinatorics of the Hamming space. *J. Combin. Theory Ser. A*, 71(1):112–126, 1995.

[KRS99] R. Kumar, S. Rajagopalan, and A. Sahai. Coding constructions for blacklisting problems without computational assumptions. In *Crypto'99*, volume 1666 of *Springer Lecture Notes in Computer Science*, pages 609–623, 1999.

[KS64] W. Kautz and R. Singleton. Nonrandom binary superimposed codes. *IEEE Trans. Inform. Theory*, 10(4):363–377, October 1964.

[KS88] J. Körner and G. Simonyi. Separating partition systems and locally different sequences. *SIAM J. Discrete Math.*, 1:355–359, 1988.

[KS02] A. Krasnopeev and Yu. L. Sagalovich. The kerdock codes and separating systems. In *Eight International Workshop on Algebraic and Combinatorial Coding Theory*, 2002.

[Lev98] Vladimir I. Levenshtein. Universal bounds for codes and designs. In *Handbook of coding theory, Vol. I*, pages 499–648. North-Holland, Amsterdam, 1998.

[MRRW77] Robert J. McEliece, Eugene R. Rodemich, Howard Rumsey, Jr., and Lloyd R. Welch. New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities. *IEEE Trans. Inform. Theory*, IT-23(2):157–166, 1977.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1977.

[NT78] T. Nanya and Y. Tohma. On universal single transition time asynchronous state assignments. *IEEE Trans. Comput.*, 27:781–782, 1978.

[PS72] M. S. Pinsker and Yu. L. Sagalovich. A lower bound on the size of automata state codes. *Problems of Information Transmission*, 8(3):59–66, 1972.

[Sag65] Yu. L. Sagalovich. A method for increasing the reliability of finite automata. *Problems of Information Transmission*, 1(2):27–35, 1965.

[Sag73] Yu. L. Sagalovich. An upper bound on the size of automata state codes. *Problems of Information Transmission*, 9(1):73–83, 1973.

[Sag75] Yu. L. Sagalovich. *State Assignment and Reliability of Automata*. Svyaz, Moscow, 1975. In Russian.

[Sag82] Yu. L. Sagalovich. Completely separating systems. *Problems of Information Transmission*, 18(2):74–82, 1982.

[Sag94] Yu. L. Sagalovich. Separating systems. *Problems of Information Transmission*, 30(2):105–123, 1994.

[Sch00] Hans Georg Schaathun. The weight hierarchy of product codes. *IEEE Trans. Inform. Theory*, 46(7):2648–2651, November 2000.

[Sch01] Hans Georg Schaathun. Upper bounds on weight hierarchies of extremal non-chain codes. *Discrete Math.*, 241(1–3):449–469, 2001.

[Sch03] Hans Georg Schaathun. Fighting two pirates. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Springer Lecture Notes in Computer Science. Springer-Verlag, 2003.

[SSW00] J. N. Staddon, D. R. Stinson, and R. Wei. Combinatorial properties of frameproof and traceability codes. Available at `http://www.cacr.math.uwaterloo.ca/~dstinson/.`, September 2000.

[STW00] D.R. Stinson, Tran Van Trung, and R. Wei. Secure frameproof codes, key distribution patterns, group testing algorithms and related structures. *J. Stat. Planning and Inference*, 86(2):595–617, 2000.

[SvTW00] D. R. Stinson, Tran van Trung, and R. Wei. Secure frameproof codes, key distribution patterns, group testing algorithms and related structures. *J. Statist. Plann. Inference*, 86(2):595–617, 2000. Special issue in honor of Professor Ralph Stanton.

[SW98] D. R. Stinson and R. Wei. Combinatorial properties and constructions of traceability schemes and frameproof codes. *SIAM J. Discrete Math.*, 11(1):41–53 (electronic), 1998.

[SWZ00] D. R. Stinson, R. Wei, and L. Zhu. New constructions for perfect hash families and related structures using combinatorial designs and codes. *J. Combin. Des.*, 8(3):189–200, 2000.

[Tsf91] Michael A. Tsfasman. Algebraic-geometric codes and asymptotic problems. *Discrete Appl. Math.*, 33(1-3):241–256, 1991. Applied algebra, algebraic algorithms, and error-correcting codes (Toulouse, 1989).

[TV95] Michael A. Tsfasman and Serge G. Vlăduţ. Geometric approach to higher weights. *IEEE Trans. Inform. Theory*, 41(6, part 1):1564–1588, 1995. Special issue on algebraic geometry codes.

[Ung69] S. H. Unger. *Asynchronous Sequential Switching Circuits*. Wiley, 1969.

[Wei91] Victor K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inform. Theory*, 37(5):1412–1418, 1991.

[Xin02] Chaoping Xing. Asymptotic bounds on frameproof codes. *IEEE Trans. Inform. Theory*, 40(11):2991–2995, November 2002.