Configuration Distribution and Designs of Codes in the Johnson Scheme

Tuvi Etzion
Technion—Israel Institute of Technology, Department of Computer Science, Technion City, Haifa 32000, Israel, E-mail: etzion@cs.technion.ac.il
Received May 8, 2005; revised December 8, 2005

Published online 15 February 2006 in Wiley InterScience (www.interscience.wiley.com).
DOI 10.1002/jcd.20102

Abstract: The main goal of this article is to present several connections between perfect codes in the Johnson scheme and designs, and provide new tools for proving Delsarte conjecture that there are no nontrivial perfect codes in the Johnson scheme. Three topics will be considered. The first is the configuration distribution which is akin to the weight distribution in the Hamming scheme. We prove that if there exists an e-perfect code $\mathcal{C}$ in the Johnson scheme then there is a formula which connects the number of vectors at distance i from any codeword in various codes isomorphic to $\mathcal{C}$. The second topic is the Steiner systems embedded in a perfect code. We prove a lower bound on the number of Steiner systems embedded in a perfect code. The last topic is the strength of a perfect code. We show two new methods for computing the strength of a perfect code and demonstrate them on 1-perfect codes. We further discuss how to settle Delsarte conjecture. © 2006 Wiley Periodicals, Inc. J Combin Designs 15: 15–34, 2007

Keywords: *Johnson scheme; k-regular code; moments; perfect codes; Steiner system; t-design*

1. INTRODUCTION

Coding theory and block design are two areas which were developed separately in parallel, but during the years these two areas had intersected in many places. The main intersections between these two areas are in constant weight codes and perfect codes.

The Johnson graph $J(n, w)$ is a graph whose set of vertices $\mathcal{V}_w^n$ consists of all $\binom{n}{w}$ w-subsets of an n-set $\mathcal{N} = \{1, 2, \ldots, n\}$. Two vertices u and v are adjacent if and only if $|u \cap v| = w - 1$. The *distance* $d(u, v)$ between two vertices u and v is the length of the shortest path which connects these vertices, that is, $d(u, v) = w - |u \cap v|$. A code $\mathcal{C}$ in

Contract grant sponsor: ISRAEL SCIENCE FOUNDATION (in Part); Contract grant number: 263/04.
© 2006 Wiley Periodicals, Inc.

$J(n, w)$ is a subset of $\mathcal{V}_w^n$. The minimum distance of $\mathcal{C}$, $d(\mathcal{C}) = minimum\{d(u, v) : u \neq v, u, v \in \mathcal{C}\}$.

A code $\mathcal{C}$ of such w-subsets is called an e-perfect code in $J(n, w)$ (or in the Johnson scheme) if the e-spheres with centers at the codewords of $\mathcal{C}$ form a partition of $\mathcal{V}_w^n$. In other words, $\mathcal{C}$ is an e-perfect code if for each element $v \in V_w^n$ there exists a unique element $c \in C$ such that the distance between v and c is at most e. Clearly, the minimum distance of an e-perfect code is $2e + 1$. There are some trivial perfect codes in $J(n, w)$:

1. V_w^n is 0-perfect.
2. Any $\{v\}$, $v \in V_w^n$, is w-perfect.
3. if $n = 2w$, w odd, any pair of disjoint w-subsets is e-perfect with $e = \frac{1}{2}(w - 1)$.

It was conjectured by Delsarte [3] that these are the only e-perfect codes in $J(n, w)$. Many attempts were made during the last 30 years to settle Delsarte conjecture, but there was only a limited success, especially as in the other important schemes there is a complete characterization of all perfect codes. The first major result is due to Roos [12] and it was slightly improved in [6].

Theorem 1. *If there exists an e-perfect code in $J(n, w)$ then $n < (w - 1)\frac{2e+1}{e}$.*

Roos has proved that $n \leq (w - 1)\frac{2e+1}{e}$ by using a modified version of the sphere packing bound and anticodes. The proof in [6] of Theorem 1 as well as the other nonexistence results were obtained by using t-designs.

A *t-design* $S_\lambda(t, w, n)$ is a collection $\mathcal{C}$ of w-subsets called *blocks* of $\mathcal{N}$, such that each t-subset of $\mathcal{N}$ is a subset of exactly λ blocks of $\mathcal{C}$. When $\lambda = 1$ the design is called a *Steiner system* and is denoted by $S(t, w, n)$. The largest t of a code $\mathcal{C}$ for which the code is a t-design is called the *strength* of the code. The existence of a t-design $S_\lambda(t, w, n)$ implies the existence of $(t - 1)$-designs $S_\lambda(t - 1, w - 1, n - 1)$ (called *the derived design*) and $S_{\lambda'}(t - 1, w, n)$, and hence it must satisfy certain well-known divisibility conditions:

Theorem 2. *A necessary condition for a t-design $S_\lambda(t, w, n)$ to exist is that the numbers $\lambda\frac{\binom{n-i}{t-i}}{\binom{w-i}{t-i}}$, must be integers, for all $0 \leq i \leq t$.*

If $\mathcal{C}$ is an e-perfect code in $J(n, w)$ then its size is

$$\frac{\binom{n}{w}}{\Phi_e(n, w)},$$

where

$$\Phi_e(n, w) = \sum_{i=0}^{e} \binom{w}{i}\binom{n-w}{i},$$

is the size of an e-sphere. If the code $\mathcal{C}$ has strength φ then for each t, $0 \leq t \leq \varphi$, it is a t-design $S_{\lambda_t}(t, w, n)$, where

$$\lambda_t = \frac{\binom{n-t}{w-t}}{\Phi_e(n, w)}. \tag{1}$$

The divisibility conditions of (1) restrict the range of parameters in which e-perfect codes can exist. We summarize some of the relevant results from [6].

Theorem 3.

- *If $\mathcal{C}$ is an e-perfect code in $J(n, w)$, $e \geq 2$, then its strength is at least $\frac{w}{e} - e - 1$.*
- *There exists W_e such that for all $w \geq W_e$, all e-perfect codes in $J(n, w)$ have strength at least $\lfloor \frac{w}{2} \rfloor$.*
- *If $e \equiv -1 (\text{mod } p^2)$, p prime, then there can be only finitely many e-perfect codes in $J(n, w)$.*
- *There are no nontrivial 3-perfect, 7-perfect, 8-perfect codes in $J(n, w)$.*

The following three theorems on the parameters in which perfect codes cannot exist due to the Steiner systems which are embedded in them are given in [4,5,6].

Theorem 4. *If there exists an e-perfect code in $J(n, w)$ then the following Steiner systems exist:*

$$S(2, e+2, w+2), \quad S(2, e+2, n-w+2),$$

$$S(e+1, 2e+1, w), \quad S(e+1, 2e+1, n-w).$$

Theorem 5. *Assume there exists an e-perfect code in $J(n, w)$.*

- *If e is odd then n is even and $(e+1)(e+2)$ divides $n - 2w$.*
- *If e is even and n is even then $(e+1)(e+2)$ divides $n - 2w$.*
- *If e is even and n is odd then $e \equiv 0 \ (\text{mod } 4)$ and $\frac{(e+1)(e+2)}{2}$ divides $n - 2w$.*

Corollary 1. *There are no perfect codes in:*

- *$J(2w + p^i, w)$, p is a prime and $i \geq 1$.*
- *$J(2w + pq, w)$, p and q primes, $q < p$, and $p \neq 2q - 1$.*

Some more similar corollaries to Corollary 1 can be obtained from Theorem 5. Other papers which examine perfect codes in the Johnson scheme include [1,2,7,14].

For a subset $\mathcal{A} \subseteq \mathcal{N}$, the *complement* $\bar{\mathcal{A}}$ is defined by $\bar{\mathcal{A}} = \mathcal{N} \setminus \mathcal{A}$. The complement of a code $\mathcal{C}$ is defined by $\bar{\mathcal{C}} = \{\bar{c} : c \in \mathcal{C}\}$. For simplicity, we usually assume that $n \geq 2w$, that is, $n = 2w + a$, as a consequence of the following simple result.

Lemma 1. *The complement of an e-perfect code in $J(n, w)$ is an e-perfect code in $J(n, n - w)$.*

The main purpose of this article is to present connections between e-perfect codes and t-design, and to present a few new tools which can be useful in settling Delsarte conjecture.

We hope that the theory presented could help in exploring properties of other constant weight codes.

The rest of this article is organized as follows. In Section 2, we introduce the concepts of configuration and configuration distribution which can be used to prove all known results on the nonexistence of e-perfect codes in $J(n, w)$. These concepts are akin to weight and weight distribution in the Hamming scheme. We prove a formula akin to the one in the Hamming scheme which states how the vectors of weight i are distributed between the various translates of a perfect code. In Section 3, we make an exact enumeration of the number of Steiner systems known to exist in an e-perfect code by Theorem 4. In Section 4, we introduce two new methods to compute the strength of a perfect code. These methods simplify the methods previously known for this computation. We summarize in Section 5 with an outline of directions how to settle Delsarte conjecture.

2. CONFIGURATION DISTRIBUTION

A code $\mathcal{C}$ in $J(n, w)$ can be described in terms of binary codewords of length n and weight w, that is, each codeword has exactly w ones. Each subset $\{i_1, i_2, \ldots, i_w\}$ is translated into a binary word of length n with w ones in positions $i_1, i_2, \ldots, i_w$. In the sequel we will use a mixed language of set notation and vector notation. It should be understood from the context which one we are using, and how to translate between the two different notations.

Let $\mathcal{C}$ be a code in $J(n, w)$. We can partition the coordinate set $\mathcal{N}$ into r subsets $\{\mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_r\}$. A vector $x \in \mathcal{V}_w^n$ can be written as $x = (x_1, x_2, \ldots, x_r)$, where $x_i \subseteq \mathcal{H}_i$, $1 \leq i \leq r$. We say that x is from configuration $(w_1, w_2, \ldots, w_r)$, $\sum_{i=1}^{r} w_i = w$, if $|x_i| = w_i$, $1 \leq i \leq r$. We denote by $D_{(w_1, w_2, \ldots, w_r)}$ the number of codewords from configuration $(w_1, w_2, \ldots, w_r)$. The *configuration distribution* of $\mathcal{C}$ is a vector consisting of all the values $D_{(w_1, w_2, \ldots, w_r)}$, where $w_i \leq |\mathcal{H}_i|$, $1 \leq i \leq r$, and $\sum_{i=1}^{r} w_i = w$.

The configuration distribution is an important parameter for examining a code in the Johnson scheme. In [13] a generalization of MacWilliams identities was given for such partitions and configuration distribution. In [4] several partitions with $r = 2$ were considered. The most important one is the one in which $|\mathcal{H}_1| = w$ and $|\mathcal{H}_2| = w + a$. Clearly, a permutation on the columns of $\mathcal{C}$ will result in an e-perfect code isomorphic to $\mathcal{C}$. In this case it was proved in [4] that an e-perfect code can have exactly $e + 1$ different configuration distributions. In order to avoid confusion we will assume that that the vector from configuration $(w, 0)$ is always a codeword in a perfect code $\mathcal{C}$. If we permute the columns of $\mathcal{C}$ (in other words, we take another partition $\{\mathcal{G}_1, \mathcal{G}_2\}$ of $\mathcal{N}$, such that $|\mathcal{G}_1| = w$ and $|\mathcal{G}_2| = w + a$) in a way that the vector from configuration $(w, 0)$ is not a codeword we will call the obtained code a *translate* of $\mathcal{C}$. For each j, $1 \leq j \leq e$, there exists a translate with exactly one *translate-word* from configuration $(w - j, j)$, and no translate-word from configuration $(w - i, i)$, $0 \leq i \leq e$, $i \neq j$; the translate-word from configuration $(w - j, j)$ will be called a translate leader. Let A_i, $0 \leq i \leq w$, be the number of codewords in configuration $(w - i, i)$ and let $B_{i,j}$, $0 \leq i \leq w$, $0 \leq j \leq e$, be the number of translate-words from configuration $(w - i, i)$ in the translate with translate-leader $(w - j, j)$. Note, that $A_i = B_{i,0}$ and $B_{i,j} = D_{(w-i,i)}$ in the corresponding translate. A_i is also the number of codewords which have distance i to the codeword from configuration $(w, 0)$ and $(A_i)_{i=0}^{w}$ is the inner distance distribution of the code in the Johnson scheme. $(B_{i,j})_{i=0}^{w}$ is the configuration distribution which is akin to the weight distribution in the Hamming scheme.

Our main theorem in this section is akin to a similar theorem in the Hamming scheme, but the proofs of both theorems are completely different.

Theorem 6. *For a given e-perfect code $\mathcal{C}$ in $J(2w+a, w)$ we have*

$$\sum_{j=0}^{e} \binom{w}{j} \binom{w+a}{j} B_{i,j} = \binom{w}{i} \binom{w+a}{i}.$$

The theorem states that the number of vectors from configuration $(w-i, i)$ are distributed between the translates, in a way that from translate with translate leader from configuration $(w-j, j)$, $0 \leq j \leq e$, we take the number of codewords from configuration $(w-i, i)$, $B_{i,j}$, and multiply by the total number of vectors from configuration $(w-j, j)$, which is $\binom{w}{j}\binom{w+a}{j}$. This does not mean that there are $\binom{w}{j}\binom{w+a}{j}$ translates with translate leader from configuration $(w-j, j)$ which are pairwise disjoint, which is the scenario in the Hamming scheme.

The proof of the theorem consists of several steps and we will break it accordingly. The proof will be by induction. Let $c \in \mathcal{C}$ be a codeword and $x \in \mathcal{V}_w^n$. We say that c ρ-cover x if $d(c, x) \leq \rho$. A code $\mathcal{C}$ ρ-cover all the elements which are ρ-covered by its codewords. We will prove that the number of vectors from configuration $(w-i, i)$, which are ρ-covered by $\mathcal{C}$ is equal to $\sum_{j=0}^{\rho} \binom{w}{j}\binom{w+a}{j} B_{i,j}$. Since $\mathcal{C}$ is an e-perfect code the theorem will follow by substituting $\rho = e$.

For the rest of this section, let $\mathcal{C}$ be an e-perfect code in $J(n, w)$. Let $\{\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3, \mathcal{H}_4\}$ be a partition of $\mathcal{N}$, such that $|\mathcal{H}_2| = |\mathcal{H}_3| = j$, $|\mathcal{H}_1| = w - j$, and $|\mathcal{H}_4| = w + a - j$, $1 \leq j \leq e+1$. Let $\{\mathcal{G}_1 = \mathcal{H}_1 \cup \mathcal{H}_2, \mathcal{G}_2 = \mathcal{H}_4 \cup \mathcal{H}_3\}$ be a partition of $\mathcal{N}$ and $\{\tilde{\mathcal{G}}_1 = \mathcal{H}_1 \cup \mathcal{H}_3, \tilde{\mathcal{G}}_2 = \mathcal{H}_4 \cup \mathcal{H}_2\}$ another partition of $\mathcal{N}$. For the next three lemmas, we use vectors from configurations of the form $(\alpha, \beta, \gamma, \delta)$ with respect to the partition $\{\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3, \mathcal{H}_4\}$.

Lemma 2. *If $D_{(w-j,j,0,0)} = 1$ then $D_{(\alpha,\beta,\gamma,\delta)}$ has a value that depends only on α, β, γ, and δ.*

Proof. We will order all the configurations and prove the lemma by induction. Given two configurations $(\alpha_i, \beta_i, \gamma_i, \delta_i)$, $i = 1, 2$, then $(\alpha_1, \beta_1, \gamma_1, \delta_1)$ is before $(\alpha_2, \beta_2, \gamma_2, \delta_2)$ in this order if one of the following holds:

- $\alpha_1 + \beta_1 > \alpha_2 + \beta_2$.
- $\alpha_1 + \beta_1 = \alpha_2 + \beta_2$ and $\alpha_1 > \alpha_2$.
- $\alpha_1 = \alpha_2$, $\beta_1 = \beta_2$, and $\delta_1 < \delta_2$.

Note, that since $D_{(w-j,j,0,0)} = 1$ it follows that $D_{(\alpha,\beta,\gamma,\delta)} = 0$ if $w - 2e - 1 < \alpha + \beta < w$. Now, we will describe the induction informally. The basis is that $D_{(w-j,j,0,0)} = 1$ and $D_{(\alpha,\beta,\gamma,\delta)} = 0$, as long as $w - 2e - 1 < \alpha + \beta < w$.

Assume that the values of $D_{(\cdot,\cdot,\cdot,\cdot)}$ for all configurations before configuration $(\alpha, \beta, \gamma, \delta)$ are known by the induction hypothesis. Therefore, all vectors from configuration (a, b, c, d) where $a + b > \alpha + \beta + e$ are e-covered by codewords from configuration before $(\alpha, \beta, \gamma, \delta)$. Vectors from configuration (a, b, c, d), where $a + b = \alpha + \beta + e$ and $a > \alpha + e$ are also e-covered by codewords from configurations before $(\alpha, \beta, \gamma, \delta)$. Finally, vectors from configuration (a, b, c, d), where $a = \alpha + e$, $b = \beta$ and $d < \delta - e$ are also e-covered by codewords from configuration before $(\alpha, \beta, \gamma, \delta)$. (Note, that $\alpha \leq \alpha + \beta \leq w - 2e - 1$, $\gamma + \delta \geq 2e + 1$, and $\delta \geq e$, which makes all the mentioned values valid.)

Vectors from configuration $(\alpha+e, \beta, \gamma, \delta-e)$ cannot be e-covered by configurations after $(\alpha, \beta, \gamma, \delta)$. Thus, all vectors from configuration $(\alpha+e, \beta, \gamma, \delta-e)$ which are not e-covered by configurations before $(\alpha, \beta, \gamma, \delta)$ must be e-covered by configuration $(\alpha, \beta, \gamma, \delta)$. Since all values $D_{(\cdot,\cdot,\cdot,\cdot)}$ which are before $(\alpha, \beta, \gamma, \delta)$ are determined by the initial values of the basis, it follows that the number of vectors from configuration $(\alpha+e, \beta, \gamma, \delta-e)$ which are not e-covered by configurations proceeding $(\alpha, \beta, \gamma, \delta)$ is determined by the initial values of the basis.

Therefore, $D_{(\alpha,\beta,\gamma,\delta)}$ has a value that depends only on α, β, γ, and δ. □

Lemma 3. *If* $D_{(w-j,j,0,0)} = 1$ *then* $D_{(\alpha,\beta,\gamma,\delta)} = \frac{\binom{\alpha+\beta}{\beta}\binom{w-\alpha-\beta}{j-\beta}\binom{\gamma+\delta}{\gamma}\binom{w+a-\gamma-\delta}{j-\gamma}}{\binom{w}{j}\binom{w+a}{j}} A_{\gamma+\delta}$

Proof. By Lemma 2 the value $D_{(\alpha,\beta,\gamma,\delta)}$ is determined since $D_{(w-j,j,0,0)} = 1$. As any j coordinates of $\mathcal{G}_1$ in the codeword from configuration $(w, 0)$ have j ones, we can exchange any such j columns with the columns of $\mathcal{H}_2$ without affecting the configuration distribution with respect to the partition with four subsets. The same arguments hold for any j coordinates of $\mathcal{G}_2$ and any combination of j coordinates of $\mathcal{G}_1$ with j coordinates of $\mathcal{G}_2$. A codeword from configuration $(\alpha, \beta, \gamma, \delta)$ with respect to $\{\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3, \mathcal{H}_4\}$, is a codeword from configuration $(\alpha+\beta, \gamma+\delta)$ with respect to $\{\mathcal{G}_1, \mathcal{G}_2\}$. The number of such codewords is $A_{\gamma+\delta}$. The coordinates of $\mathcal{H}_2$ must consist of β ones with respect to these codewords, and similarly the coordinates of $\mathcal{H}_3$ must consist of γ ones. Hence, there are $\binom{\alpha+\beta}{\beta}\binom{w-\alpha-\beta}{j-\beta}\binom{\gamma+\delta}{\gamma}\binom{w+a-\gamma-\delta}{j-\gamma}$ ways to distribute the zeroes and the ones of each codeword. Summing on all the codewords from configuration $(\alpha+\beta, \gamma+\delta)$ we have $\binom{\alpha+\beta}{\beta}\binom{w-\alpha-\beta}{j-\beta}\binom{\gamma+\delta}{\gamma}\binom{w+a-\gamma-\delta}{j-\gamma} A_{\gamma+\delta}$. As these must be distributed equally between all choices of j coordinates of $\mathcal{G}_1$ and each j coordinates of $\mathcal{G}_2$, as a consequence of Lemma 2, we obtain

$$D_{(\alpha,\beta,\gamma,\delta)} = \frac{\binom{\alpha+\beta}{\beta}\binom{w-\alpha-\beta}{j-\beta}\binom{\gamma+\delta}{\gamma}\binom{w+a-\gamma-\delta}{j-\gamma}}{\binom{w}{j}\binom{w+a}{j}} A_{\gamma+\delta}. \tag{2}$$

□

Lemma 4. *For a given* j, $1 \le j \le e$,

$$\begin{aligned}\binom{w}{j}\binom{w+a}{j} B_{i,j} = \sum_{r=0}^{j}\sum_{s=0}^{j} &\binom{w-i-r+s}{s}\binom{i+r-s}{j-s}\binom{i-s+r}{r} \\ &\times \binom{w+a-i-r+s}{j-r} A_{i-s+r}\end{aligned} \tag{3}$$

Proof. A translate with translate-leader from configuration $(w-j, j)$ is formed by using the partition $\{\tilde{\mathcal{G}}_1, \tilde{\mathcal{G}}_1\}$ instead of the partition $\{\mathcal{G}_1, \mathcal{G}_2\}$, that is, exchanging between $\mathcal{H}_2$ and $\mathcal{H}_3$ in the partition. Note, that $B_{i,j}$ denote the number of translate-words from configuration $(w-i, i)$ with respect to the partition $\{\tilde{\mathcal{G}}_1, \tilde{\mathcal{G}}_2\}$. Therefore, any codeword from configuration

$(w-i-r, s, r, i-s)$ will become a translate-word from configuration $(w-i, i)$. Hence, by using Lemma 3 we have

$$B_{i,j} = \sum_{r=0}^{j}\sum_{s=0}^{j} D_{(w-i-r,s,r,i-s)}$$
$$= \frac{\sum_{r=0}^{j}\sum_{s=0}^{j}\binom{w-i-r+s}{s}\binom{i+r-s}{j-s}\binom{i-s+r}{r}\binom{w+a-i-r+s}{j-r}}{\binom{w}{j}\binom{n-w}{j}} A_{i-s+r}$$

which implies the claim of the lemma. □

The next step is to consider how the $\binom{w}{i}\binom{w+a}{i}$ vectors from configuration $(w-i, i)$ are covered by the codewords of $\mathcal{C}$. In the sequel we say that the codeword $c \in \mathcal{C}$ *ρ-exact-cover* the vector x if $d(c, x) = \rho$.

Lemma 5.

- *Vectors from configuration* $(w-i, i)$ *are* ρ*-exact-covered only by codewords from configurations* $(w-i-r, i+r)$ *and* $(w-i+r, i-r)$, $0 \le r \le \rho$.
- *For a given* r, $0 \le r \le \rho$, *the number of vectors from configuration* $(w-i, i)$ *which are* ρ*-exact-covered by codewords from configuration* $(w-i-r, i+r)$ *is*

$$\sum_{s=r}^{\rho}\binom{i+r}{s}\binom{w+a-i-r}{s-r}\binom{w-i-r}{\rho-s}\binom{i+r}{\rho-s+r} A_{i+r} \tag{4}$$

Proof. The first claim of the lemma is trivial. As for the second claim, let $c \in \mathcal{C}$ be a codeword from configuration $(w-i-r, i+r)$. If for a vector x from configuration $(w-i, i)$ we have $d(c, x) = \rho$ then c and x must differ in at least r coordinates and in at most ρ coordinates of $\mathcal{G}_2$, in which c has ones. Assume they differ in s coordinates, $r \le s \le \rho$. Therefore, they must differ in exactly $s-r$ coordinates of $\mathcal{G}_2$ in which c has zeroes. As $d(c, x) = \rho$ they must differ in exactly $\rho - s$ coordinates of $\mathcal{G}_1$, in which c has ones, and $\rho - s + r$ coordinates of $\mathcal{G}_1$, in which c has zeroes. The second claim of the lemma follows from these arguments. □

Similarly we have the following lemma.

Lemma 6. *For a given* r, $0 \le r \le \rho$, *the number of vectors from configuration* $(w-i, i)$ *which are* ρ*-exact-covered by codewords from configuration* $(w-i+r, i-r)$ *is*

$$\sum_{s=r}^{\rho}\binom{i-r}{s-r}\binom{w+a-i+r}{s}\binom{w-i+r}{\rho-s+r}\binom{i-r}{\rho-s} A_{i-r} \tag{5}$$

For a given ρ, $0 \le \rho \le e$, let $\mathcal{N}(i, \mathcal{C}, \rho)$ be the number of vectors from configuration $(w-i, i)$ which are ρ-covered by $\mathcal{C}$.

Lemma 7. *Let $\mathcal{C}$ be an e-perfect code in $J(n, w)$. The number of vectors from configuration $(w-i, i)$ which are ρ-covered by $\mathcal{C}$ is*

$$\mathcal{N}(i,\mathcal{C},\rho)=\mathcal{N}(i,\mathcal{C},\rho-1)+\sum_{r=1}^{\rho}\sum_{s=r}^{\rho}\binom{i-r}{s-r}\binom{w+a-i+r}{s}\binom{w-i+r}{\rho-s+r}\binom{i-r}{\rho-s}A_{i-r}$$
$$+\sum_{r=0}^{\rho}\sum_{s=r}^{\rho}\binom{i+r}{s}\binom{w+a-i-r}{s-r}\binom{w-i-r}{\rho-s}\binom{i+r}{\rho-s+r}A_{i+r}$$

Proof. The lemma follows immediately from the definition of $\mathcal{N}(i, \mathcal{C}, \rho)$, Lemmas 5 and 6, by summing Equations (4) and (5) for values of r in the equations (note, that $r = 0$ relates to the same vectors in both equations). □

Theorem 7. *For any given ρ, $0 \le \rho \le e$,*

$$\sum_{r=0}^{\rho}\binom{w}{r}\binom{w+a}{r}B_{i,r}=\mathcal{N}(i,\mathcal{C},\rho). \tag{6}$$

Proof. The proof is by induction on ρ.

Basis. For $\rho = 0$ the left side of Equation (6) is $B_{i,0}$. The right side of Equation (6) is equal to the number of vectors from configuration $(w-i, i)$ which are 0-covered by $\mathcal{C}$, which is obviously the number of codewords from configuration $(w-i, i)$, that is, A_i. By definition $B_{i,0} = A_i$.

Induction hypothesis. Assume the claim is true for $\rho - 1$.

Induction step. We will prove that the claim is true for ρ. By the induction hypothesis and Lemma 7 we only have to prove that

$$\binom{w}{\rho}\binom{w+a}{\rho}B_{i,\rho}=\sum_{m=1}^{\rho}\sum_{s=m}^{\rho}\binom{i-m}{s-m}\binom{w+a-i+m}{s}\binom{w-i+m}{\rho-s+m}\binom{i-m}{\rho-s}A_{i-m}$$
$$+\sum_{m=0}^{\rho}\sum_{s=m}^{\rho}\binom{i+m}{s}\binom{w+a-i-m}{s-m}\binom{w-i-m}{\rho-s}\cdot\binom{i+m}{\rho-s+m}A_{i+m}. \tag{7}$$

By Equation (3) we have that the coefficient of A_{i+m} in the expansion of $\binom{w}{\rho}\binom{w+a}{\rho}B_{i,\rho}$, which is obtained by substituting $r = s + m$, is $\sum_{s=0}^{\rho-m}\binom{w-i-m}{s}\binom{i+m}{\rho-s}\binom{i+m}{s+m}\binom{w+a-i-m}{\rho-s-m}$. It is equal to $\sum_{s'=m}^{\rho}\binom{w-i-m}{\rho-s'}\binom{i+m}{s'}\binom{i+m}{\rho-s'+m}\binom{w+a-i-m}{s'-m}$ after substituting $s' = \rho - s$, which is equal to the coefficient of A_{i+m} in (7). The same arguments hold for the coefficients of A_{i-m} in (3) and (7). Hence, the induction step and the theorem are proved. □

Proof of Theorem 6. By taking $\rho = e$ in Theorem 7 we obtain

$$\sum_{r=0}^{e}\binom{w}{r}\binom{w+a}{r}B_{i,r}=\mathcal{N}(i,\mathcal{C},e).$$

Since $\mathcal{C}$ is a perfect code, it follows that $\mathcal{N}(i, \mathcal{C}, e) = \binom{w}{i}\binom{w+a}{i}$ and hence

$$\sum_{r=0}^{e} \binom{w}{r}\binom{w+a}{r} B_{i,r} = \binom{w}{i}\binom{w+a}{i}.$$

□

Remark. An alternative way to prove Theorem 6 is to partition $\mathcal{N}$ into two subsets $\mathcal{G}_1$ and $\mathcal{G}_2$ such that $|\mathcal{G}_1| = w$ and $|\mathcal{G}_2| = w + a$. We consider the codewords from the first configurations with codewords in the translates of $\mathcal{C}$. Induction should be used with the observation that each vector from configuration $(w - i, i)$ should be e-covered a total of exactly $\Phi_e(n, w)$ times by $\mathcal{C}$ and its $\Phi_e(n, w) - 1$ translates.

3. STEINER SYSTEMS IN A PERFECT CODE

Assume an e-perfect code $\mathcal{C}$ exists in $J(n, w)$. We say that a Steiner system $S(t, k, v)$ is embedded in $\mathcal{C}$ if there exists a set of codewords $\mathcal{C}_1 \subseteq \mathcal{C}$ and a set of coordinates $\mathcal{M} \subseteq \mathcal{N}$, $|\mathcal{M}| = v$, such that $\{c \cap \mathcal{M} : c \in \mathcal{C}_1\}$ is a Steiner system $S(t, k, v)$. By Theorem 4, the existence of an e-perfect code in $J(n, w)$ implies the existence of the Steiner systems $S(e + 1, 2e + 1, w)$, $S(e + 1, 2e + 1, n - w)$, $S(2, e + 2, w + 2)$, and $S(2, e + 2, n - w + 2)$. These Steiner systems are embedded either in $\mathcal{C}$ or in $\bar{\mathcal{C}}$. In this section we examine how many systems of these types are embedded in $\mathcal{C}$ and $\bar{\mathcal{C}}$.

Let's examine first the Steiner systems $S(e + 1, 2e + 1, w)$ and $S(e + 1, 2e + 1, n - w)$. Let $\{\mathcal{H}_1, \mathcal{H}_2\}$ be a partition of $\mathcal{N}$ such that $|\mathcal{H}_1| = w$, $|\mathcal{H}_2| = n - w$, and the vector from configuration $(w, 0)$ is a codeword. The vectors which are e-covered by this codeword are vectors from all configurations of the form $(w - i, i), 0 \leq i \leq e$. Since the minimum distance of $\mathcal{C}$ is $2e + 1$, it follows that there are no codewords from configurations $(w - i, i), 1 \leq i \leq 2e$. There are $\binom{w}{e+1}\binom{n-w}{e+1}$ vectors in configuration $(w - e - 1, e + 1)$. These vectors must be e-exact-covered by codewords from configuration $(w - 2e - 1, 2e + 1)$. Each codeword from configuration $(w - 2e - 1, 2e + 1)$ e-covers $\binom{2e+1}{e}\binom{2e+1}{e}$ words from configuration $(w - e - 1, e + 1)$ and therefore, there are $\frac{\binom{w}{e+1}\binom{n-w}{e+1}}{\binom{2e+1}{e}\binom{2e+1}{e}}$ codewords from configuration $(w - 2e - 1, 2e + 1)$.

Consider a subset $\mathcal{G}_1$ of $\mathcal{H}_1$ with size $e + 1$. Consider now all $\binom{n-w}{e+1}$ vectors in configuration $(w - e - 1, e + 1)$ which have zeroes in all coordinates of $\mathcal{G}_1$. These vectors are e-covered by codewords from configuration $(w - 2e - 1, 2e + 1)$ with zeroes in the coordinates of $\mathcal{G}_1$. Let $\mathcal{C}_1$ be this set of codewords. For each $e + 1$ coordinates of $\mathcal{H}_2$ there must be exactly one codeword from $\mathcal{C}_1$ with ones in these coordinates. Hence, $\{c \cap \mathcal{H}_2 : c \in \mathcal{C}_1\}$ is a Steiner system $S(e + 1, 2e + 1, n - w)$. Each different choice of $\mathcal{H}_1$ and $\mathcal{G}_1$ will produce a different Steiner system $S(e + 1, 2e + 1, n - w)$. Therefore, we have:

Theorem 8. *If $\mathcal{C}$ is an e-perfect code in $J(n, w)$ then there are $|\mathcal{C}|\binom{w}{e+1}$ different Steiner systems $S(e + 1, 2e + 1, n - w)$ embedded in $\mathcal{C}$.*

Corollary 2. *If $\mathcal{C}$ is an e-perfect code in $J(n, w)$ then there are $|\mathcal{C}|\binom{n-w}{e+1}$ different Steiner systems $S(e+1, 2e+1, w)$ embedded in $\bar{\mathcal{C}}$.*

We examine now the Steiner systems $S(2, e+2, w+2)$ and $S(2, e+2, n-w+2)$. Assume an e-perfect code $\mathcal{C}$ exists in $J(n, w)$. Let $\{\mathcal{G}_1, \mathcal{G}_2\}$ be a partition of $\mathcal{N}$, such that $|\mathcal{G}_1| = n-w$ and $|\mathcal{G}_2| = w$, and there is a codeword from configuration $(0, w)$. We can choose any e coordinates of $\mathcal{G}_1$ and exchange them with any e coordinates of $\mathcal{G}_2$ to obtain a partition $\{\tilde{\mathcal{G}}_1, \tilde{\mathcal{G}}_2\}$ of $\mathcal{N}$, such that $|\tilde{\mathcal{G}}_1| = n-w$, $|\tilde{\mathcal{G}}_2| = w$, and there is a codeword c_1 from configuration $(e, w-e)$. Let $\mathcal{F}_1 \subset \tilde{\mathcal{G}}_1$, $\mathcal{F}_2 \subset \tilde{\mathcal{G}}_2$, be the sets of e coordinates which were exchanged between $\mathcal{G}_2$ and $\mathcal{G}_1$, respectively. The codeword c_1 e-covers the vector from configuration $(0, w)$ and some vectors from configuration $(1, w-1)$. The vectors from configuration $(1, w-1)$ which are not e-covered by c_1 are all the vectors with exactly a single one in the coordinates of $\tilde{\mathcal{G}}_1 \setminus \mathcal{F}_1$, and exactly a single zero in the coordinates of $\tilde{\mathcal{G}}_2 \setminus \mathcal{F}_2$. There are exactly $(n-w-e)(w-e)$ such vectors from configuration $(1, w-1)$. These vectors can be e-covered only by codewords from configuration $(e+1, w-e-1)$. Each codeword from configuration $(e+1, w-e-1)$ e-exact-covers $(e+1)^2$ vectors from configuration $(1, w-1)$ and hence there are $\frac{(n-w-e)(w-e)}{(e+1)^2}$ codewords from configuration $(e+1, w-e-1)$. Let $\mathcal{C}_1$ be this set of codewords. Since the distance between any two codewords is at least $2e+1$, it follows that two codewords from configuration $(e+1, w-e-1)$ can have at most a single zero in common in $\tilde{\mathcal{G}}_2 \setminus \mathcal{F}_2$ (note, that all the $e+1$ zeroes in $\tilde{\mathcal{G}}_2$ must be in $\tilde{\mathcal{G}}_2 \setminus \mathcal{F}_2$). Therefore, there are $\binom{w-e}{2} - \frac{(n-w-e)(w-e)}{(e+1)^2}\binom{e+1}{2}$ pairs of coordinates in $\tilde{\mathcal{G}}_2 \setminus \mathcal{F}_2$ which do not have pairs of zeroes in the the codewords of $\mathcal{C}_1$ (note, that $\binom{w-e}{2} - \frac{(n-w-e)(w-e)}{(e+1)^2}\binom{e+1}{2} > 0$ is equivalent to $n < (w-1)\frac{2e+1}{e}$ which is true by Theorem 1). Any such two coordinates from $\tilde{\mathcal{G}}_2 \setminus \mathcal{F}_2$ can be joined to $\tilde{\mathcal{G}}_1$ to obtain a partition $\{\mathcal{H}_1, \mathcal{H}_2\}$ of $\mathcal{N}$, such that $|\mathcal{H}_1| = n-w+2$, $|\mathcal{H}_2| = w-2$, and there is no codeword from configuration $(i, w-2-i)$, $0 \le i \le e+1$. The vectors from configuration $(2, w-2)$ must be e-covered by codewords from configuration $(e+2, w-e-2)$. Let $\mathcal{C}_2$ be this set of codewords. Hence, $\{c \cap \mathcal{H}_1 : c \in \mathcal{C}_2\}$ is a Steiner system $S(2, e+2, n-w+2)$. We can obtain such a system by starting from any codewords of $\mathcal{C}$ and hence we have obtained $|\mathcal{C}|\binom{n-w}{e}\binom{w}{e}(\binom{w-e}{2} - \frac{(n-w-e)(w-e)}{(e+1)^2}\binom{e+1}{2})$ such Steiner systems.

We now examine whether a Steiner system $S(2, e+2, n-w+2)$ obtained by this method can be obtained in two different ways. Let $\{\mathcal{H}_1, \mathcal{H}_2\}$ be a partition of $\mathcal{N}$, such that $|\mathcal{H}_1| = n-w+2$, $|\mathcal{H}_2| = w-2$, and there is no codeword from configuration $(i, w-2-i)$, $0 \le i \le e+1$. There are $\binom{n-w+2}{2}$ vectors in configuration $(2, w-2)$. These vectors must be e-exact-covered by codewords from configuration $(e+2, w-e-2)$. Each codeword from configuration $(e+2, w-e-2)$ e-exact-covers $\binom{e+2}{e}$ words from configuration $(2, w-2)$ and therefore, there are $\frac{\binom{n-w+2}{2}}{\binom{e+2}{e}}$ codewords from configuration $(e+2, w-e-2)$. Let c_1 be a codeword from configuration $(e+2, w-e-2)$, and let $\mathcal{F}_1 = c_1 \cap \mathcal{H}_1$, and $\mathcal{F}_2 = \mathcal{H}_2 \setminus (c_1 \cap \mathcal{H}_2)$. Clearly, $|\mathcal{F}_1| = e+2$ and $|\mathcal{F}_2| = e$. We exchange the coordinates of $\mathcal{F}_1$ and $\mathcal{F}_2$ to obtain $\mathcal{G}_1 = (\mathcal{H}_1 \setminus \mathcal{F}_1) \cup \mathcal{F}_2$ and $\mathcal{G}_2 = (\mathcal{H}_2 \setminus \mathcal{F}_2) \cup \mathcal{F}_1$. It is easy to verify that $|\mathcal{G}_1| = n-w$ and $|\mathcal{G}_2| = w$, and there is a codeword from configuration $(0, w)$. Thus, each Steiner system $S(2, e+2, n-w+2)$ is obtained exactly $\frac{\binom{n-w+2}{2}}{\binom{e+2}{e}}$ times. Therefore, we have

Theorem 9. *If $\mathcal{C}$ is an e-perfect code in $J(n, w)$ then there are*

$$|\mathcal{C}|\frac{\binom{n-w}{e}\binom{w}{e}\left(\binom{w-e}{2}-\frac{(n-w-e)(w-e)}{(e+1)^2}\binom{e+1}{2}\right)\binom{e+2}{e}}{\binom{n-w+2}{2}}$$

different Steiner systems $S(2, e+2, n-w+2)$ embedded in $\mathcal{C}$.

Corollary 3. *If $\mathcal{C}$ is an e-perfect code in $J(n, w)$ then there are*

$$|\mathcal{C}|\frac{\binom{n-w}{e}\binom{w}{e}\left(\binom{n-w-e}{2}-\frac{(n-w-e)(w-e)}{(e+1)^2}\binom{e+1}{2}\right)\binom{e+2}{e}}{\binom{w+2}{2}}$$

different Steiner systems $S(2, e+2, w+2)$ embedded in $\bar{\mathcal{C}}$.

Theorems 8 and 9 and Corollaries 2 and 3 enumerate the number of Steiner systems known to exist in an e-perfect code in $J(n, w)$ by Theorem 4. Clearly, all these Steiner systems have derived Steiner systems and their enumeration can be derived from Theorems 8 and 9 and Corollaries 2 and 3.

4. THE STRENGTH OF A PERFECT CODE

What is the strength of an e-perfect code in $J(n, w)$? One method was given by Martin [9]. Martin has proved that the derived design on an e-perfect code is a completely regular code. Hence, the Lloyd theorem can be applied to this code. For the original code the Lloyd polynomial has $e+1$ integer roots, and for the new code the Lloyd polynomial has $2e+1$ integer roots. Martin proved that for $e = 1$ it implies that $w = rs+1$, $n = 2rs+r-s+1$, and the strength of the code is $s(r-1)$. A second different method was introduced in [6]. The main results are given in Theorem 3. We will describe now two methods to find the strength of the code. We will demonstrate the methods on 1-perfect codes, but the generalization for e-perfect code, $e > 1$ is straightforward, although the equations become more complicated and hence the computation of the strength is more complicated.

A. Moments

We will define a generalization for *moments* of a code which was given for the Hamming scheme [10]. Let $\mathcal{C}$ be an e-perfect code in $J(n, w)$ and let $\{\mathcal{H}_1, \mathcal{H}_2\}$ be a partition of $\mathcal{N}$ such that $|\mathcal{H}_1| = k$, $|\mathcal{H}_2| = n-k$. Let A_i be the number of codewords from configuration $(i, w-i)$ (note, that this definition is slightly different from the one of Section 2). Let $\{\mathcal{G}_1, \mathcal{G}_2\}$ be a partition of $\mathcal{N}$ such that $|\mathcal{G}_1| = k$, $|\mathcal{G}_2| = n-k$, and let B_i be the number of codewords from configuration $(i, w-i)$ with respect to this partition. The r-th *power moment*, $0 \le r$, of $\mathcal{C}$ with respect to these partitions is defined by

$$\sum_{i=0}^{k} i^r A_i, \quad \sum_{i=0}^{k} i^r B_i$$

and the r-th *binomial moment*, $0 \leq r$, of $\mathcal{C}$ is defined by

$$\sum_{i=0}^{k} \binom{i}{r} A_i, \quad \sum_{i=0}^{k} \binom{i}{r} B_i.$$

We define the *difference configuration distributions* between the two partitions by $\Delta_i = A_i - B_i$, $0 \leq i \leq k$. The r-th power moments and the r-th binomial moments with respect to the difference configuration distributions are defined by

$$\sum_{i=0}^{k} i^r \Delta_i, \quad \sum_{i=0}^{k} \binom{i}{r} \Delta_i.$$

The *Stirling number of the second kind* $S(r, v)$, $r \geq v \geq 0$, plays an important role in the connections between the two types of moments. $S(r, v)$ is the number of ways to partition r distinct objects into v identical cells, such that no cell left empty. The following three formulas are well known [11]:

$$S(r, v) = \frac{1}{v} \sum_{j=0}^{n} (-1)^{v-j} \binom{v}{j} j^r,$$

$$S(r, v) = S(r-1, v-1) + vS(r-1, v),$$

where $S(r, r) = 1$ and S(r,0)=0 for $r > 0$,

$$i^r = \sum_{v=0}^{r} v! \binom{i}{v} S(r, v)\ .$$

Hence,

$$i^r \Delta_i = \sum_{v=0}^{r} v! \binom{i}{v} S(r, v) \Delta_i\ ,$$

so that

$$\sum_{i=0}^{k} i^r \Delta_i = \sum_{i=0}^{k} \sum_{v=0}^{r} v! \binom{i}{v} S(r, v) \Delta_i = \sum_{v=0}^{r} v! S(r, v) \sum_{i=0}^{k} \binom{i}{v} \Delta_i.$$

Therefore, we can prove by induction that

Theorem 10. *For a given integer t, $\sum_{i=0}^{k} i^r \Delta_i = 0$ for all $0 \le r \le t$ if and only if $\sum_{i=0}^{k} \binom{i}{r} \Delta_i = 0$ for all $0 \le r \le t$.*

When $r \le \varphi$, the values of the binomial moments can be computed easily.

Lemma 8. *If $\mathcal{C}$ is a perfect code in $J(n, w)$ and φ is its strength then for each r, $0 \le r \le \varphi$ we have*

$$\sum_{i=0}^{k} \binom{i}{r} A_i = \sum_{i=0}^{k} \binom{i}{r} B_i = \binom{k}{r} \frac{\binom{n-r}{w-r}}{\Phi_e(n, w)}.$$

Proof. Given any integer r, it is easy to verify that $\sum_{i=0}^{k} \binom{i}{r} A_i$ is just an enumeration of the total of r-tuples with r ones in $\mathcal{H}_1$. If $r \le \varphi$ then this number does not depend on the partition as the code is an r-design. Therefore $\sum_{i=0}^{k} \binom{i}{r} A_i = \sum_{i-0}^{k} \binom{i}{r} B_i$ is just the number of ways to choose r columns out of $\mathcal{H}_1$ (or $\mathcal{G}_1$) and multiply it by the number of all-ones r-tuples in these r columns which is given in Equation (1). □

Corollary 4. *If $\mathcal{C}$ is a perfect code in $J(n, w)$ and φ is its strength then for each r, $0 \le r \le \varphi$ we have $\sum_{i=0}^{k} \binom{i}{r} \Delta_i = 0$.*

Corollary 5. *If $\mathcal{C}$ is a perfect code in $J(n, w)$ and φ is its strength then for each r, $0 \le r \le \varphi$ we have $\sum_{i=0}^{k} i^r \Delta_i = 0$.*

As said before, for simplicity, we continue our discussion with a 1-perfect code $\mathcal{C}$. By considering how the $\binom{k}{i}\binom{2w+a-k}{w-i}$ vectors from configuration $(i, w-i)$ are 1-covered by $\mathcal{C}$ we obtain the following lemma.

Lemma 9. *For any i, $0 \le i \le k$, we have*

$$\begin{aligned}&(i+1)(w+a-k+i+1)A_{i+1} + [1 + i(k-i) + (w-i)(w+a-k+i)]A_i \\ &\quad +(k-i+1)(w-i+1)A_{i-1} = \binom{k}{i}\binom{2w+a-k}{w-i}\end{aligned}$$

$$\begin{aligned}&(i+1)(w+a-k+i+1)B_{i+1} + [1 + i(k-i) + (w-i)(w+a-k+i)]B_i \\ &\quad +(k-i+1)(w-i+1)B_{i-1} = \binom{k}{i}\binom{2w+a-k}{w-i},\end{aligned}$$

where $A_j = B_j = 0$ for $j < 0$ and $j > k$.

Corollary 6. *For any i, $0 \le i \le k$, we have*

$$\begin{aligned}&(i+1)(w+a-k+i+1)\Delta_{i+1} + [1 + i(k-i) + (w-i)(w+a-k+i)]\Delta_i \\ &\quad +(k-i+1)(w-i+1)\Delta_{i-1} = 0 \qquad (8)\end{aligned}$$

We multiply the two sides of Equation (8) by i^r to obtain

$$i^r(i+1)(w+a-k+i+1)\Delta_{i+1} + i^r[1+i(k-i)+(w-i)(w+a-k+i)]\Delta_i \\ +i^r(k-i+1)(w-i+1)\Delta_{i-1} = 0,$$

which is equivalent to

$$0 = i^r(i+1)^2\Delta_{i+1} + (w+a-k)i^r(i+1)\Delta_{i+1} - 2i^{r+2}\Delta_i + (2k-a)i^{r+1}\Delta_i \\ +(w(w+a-k)+1)i^r\Delta_i + kwi^r\Delta_{i-1} - (w+k)i^r(i-1)\Delta_{i-1} + i^r(i-1)^2\Delta_{i-1}.$$

We sum for all i and obtain

$$0 = \sum_{i=-1}^{k+1} i^r(i+1)^2\Delta_{i+1} + (w+a-k)\sum_{i=-1}^{k+1} i^r(i+1)\Delta_{i+1} - 2\sum_{i=-1}^{k+1} i^{r+2}\Delta_i \\ +(2k-a)\sum_{i=-1}^{k+1} i^{r+1}\Delta_i + (w(w+a-k)+1)\sum_{i=-1}^{k+1} i^r\Delta_i + kw\sum_{i=-1}^{k+1} i^r\Delta_{i-1} \\ -(w+k)\sum_{i=-1}^{k+1} i^r(i-1)\Delta_{i-1} + \sum_{i=-1}^{k+1} i^r(i-1)^2\Delta_{i-1} \tag{9}$$

We use now the well-known binomial theorem

$$i^r = (i+1-1)^r = \sum_{j=0}^{r}(-1)^j\binom{r}{j}(i+1)^{r-j} \tag{10}$$

$$i^r = (i-1+1)^r = \sum_{j=0}^{r}\binom{r}{j}(i-1)^{r-j} \tag{11}$$

and obtain from (9), (10), and (11).

$$\sum_{s=0}^{r+2} c_s \sum_{i=-1}^{k+1} i^s\Delta_i = 0. \tag{12}$$

where $c_{r+1} = c_{r+2} = 0$ and $c_r = r^2 - (2w+a+1)r + (w^2+wa+1)$.

Now, if we assume that $\varphi = r-1$ then by Corollary 5 we have $\sum_{i=-1}^{k+1} i^s\Delta_i = 0$ for $0 \le s \le \varphi$, that is, $c_s = 0$ for $0 \le s \le \varphi$. Therefore, we must have either $c_r = 0$ or $\sum_{i=-1}^{k+1} i^r\Delta_i = \sum_{i=0}^{k} i^r\Delta_i = 0$. If $c_r \neq 0$ then $\sum_{i=0}^{k} i^r\Delta_i = 0$ and by Theorem 10 we have $\sum_{i=0}^{k}\binom{i}{r}\Delta_i = 0$. As this result does not depend on k, we can take $k = r$ and obtain that $0 = \sum_{i=0}^{k}\binom{i}{k}\Delta_i = \Delta_k$, i.e., $A_k = B_k$. As A_k and B_k are arbitrary partitions, it implies that the strength of the code is at least $k = r$, a contradiction. Thus, $c_r = 0$. Therefore we have.

Theorem 11. *If a 1-perfect code exists in $J(2w + a, w)$, then its strength is φ, where*

$$\varphi = \frac{2w + a - 1 - \sqrt{(a+1)^2 + 4(w-1)}}{2}. \tag{13}$$

Proof. By solving the quadratic equation $c_r = r^2 - (2w + a + 1)r + (w^2 + wa + 1) = 0$ the theorem is proved. □

Theorem 11 is consistent with the results of Martin [9]. In [4] it was proved that $w \equiv w + a \equiv 1 (\text{mod } 6)$ and hence $a = 2\alpha$ and to obtain an integer solution $\sqrt{(a+1)^2 + 4(w-1)}$ must be odd, that is, $\sqrt{(a+1)^2 + 4(w-1)} = 2\beta + 1$. Solving this equation we obtain that $w = (\beta - \alpha)(\beta + \alpha + 1) + 1$, $n = 2(\beta - \alpha)(\beta + \alpha + 1) + 2\alpha + 2$, and $\varphi = (\beta - \alpha)(\beta + \alpha)$.

B. t-Regular Codes

Etzion and Schwartz [6] have introduced the concept of t-regular codes.

Definition 1. *Let $\mathcal{C}$ be a code in $J(n, w)$ and let $\mathcal{A}$ be a subset of the coordinate set $\mathcal{N}$. For $0 \le i \le |\mathcal{A}|$ we define*

$$\mathcal{C}_{\mathcal{A}}(i) = |\{c \in \mathcal{C} : |c \cap \mathcal{A}| = i\}|$$

Also, for each $I \subset \mathcal{A}$ we define

$$\mathcal{C}_{\mathcal{A}}(I) = |\{c \in \mathcal{C} : c \cap \mathcal{A} = I\}|$$

Definition 2. *A code $\mathcal{C}$ in $J(n, w)$ is said to be t-regular, if the following two conditions hold:*

- **(c.1)** *There exist numbers $\alpha(0), \ldots, \alpha(t)$ such that if $\mathcal{A} \subset \mathcal{N}$, $|\mathcal{A}| = t$, then $\mathcal{C}_{\mathcal{A}}(i) = \alpha(i)$ for all $0 \le i \le t$.*
- **(c.2)** *For any given t-subset $\mathcal{A}$ of $\mathcal{N}$, there exist numbers $\beta_{\mathcal{A}}(0), \ldots, \beta_{\mathcal{A}}(t)$ such that if $I \subset \mathcal{A}$ then $\mathcal{C}_{\mathcal{A}}(I) = \beta_{\mathcal{A}}(|I|)$.*

Theorem 12. *A code $\mathcal{C}$ in $J(n, w)$ is t-regular if and only if it forms a t-design.*

Proof. Let $\mathcal{C}$ be a code in $J(n, w)$.

- If $\mathcal{C}$ is t-regular then clearly by (c.1) the code is a t-design $S_\lambda(t, w, n)$, where $\lambda = \alpha(t)$.
- If the code is a t-design $S_\lambda(t, w, n)$ then one can verify that the code is t-regular, where (c.2) holds with $\beta_{\mathcal{A}}(i) = \binom{n-t}{w-i} / \Phi_e(n, w)$, for each $0 \le i \le t$ in (c.2) which also validates (c.1).

□

The following result was proved in [6]:

Lemma 10. *If $\mathcal{C}$ is an e-perfect code in $J(n, w)$ with strength φ then property (c.2) holds for subsets of size $\varphi + 1$.*

There are two advantages for the definition of t-regular codes. The first one is that it leads to a method for computing the strength of the code [6]. In this method we use set of equations

which connect properties (c.1) and (c.2) and covering vectors of some configurations. The second is the validity of (c.2) as implied by Lemma 10. This property can be used for further investigation of the code.

Let $\mathcal{C}$ be an e-perfect code in $J(n, w)$ and let $\{\mathcal{H}_1, \mathcal{H}_2\}$, $\{\mathcal{G}_1, \mathcal{G}_2\}$, be two partitions of $\mathcal{N}$, such that $|\mathcal{H}_1| = |\mathcal{G}_1| = \varphi + 1$, $|\mathcal{H}_2| = |\mathcal{G}_2| = n - w - \varphi - 1$, where φ is the strength of the code. Furthermore, let $(A_i)_{i=0}^{\varphi+1}$, $(B_i)_{i=0}^{\varphi+1}$ be the configuration distributions and $\Delta_i = A_i - B_i$, $0 \le i \le \varphi + 1$, is the difference configuration distribution.

Lemma 11. *There exist a constant γ such that $\Delta_i = \gamma(-1)^i \binom{\varphi+1}{i}$ for all i, $0 \le i \le \varphi + 1$.*

Proof. The proof is by induction on i.

Basis. For $i = 0$, let $\gamma = \Delta_0$ and the basis is trivial.

Induction hypothesis. Assume that $\Delta_i = A_i - B_i = \gamma(-1)^i \binom{\varphi+1}{i}$, $0 \le i \le \varphi$.

Induction step. Let $\tilde{\mathcal{H}}_1 \subset \mathcal{H}_1$ and $\tilde{\mathcal{G}}_1 \subset \mathcal{G}_1$ two subsets such that $|\tilde{\mathcal{H}}_1| = |\tilde{\mathcal{G}}_1| = \varphi$. By property (c.1) we have that $\mathcal{C}_{\tilde{\mathcal{H}}_1}(i) = \mathcal{C}_{\tilde{\mathcal{G}}_1}(i)$. Since φ is the strength of the code, it follows by Lemma 10 that property (c.2) still holds for $\varphi + 1$, and hence

$$\frac{\mathcal{C}_{\tilde{\mathcal{H}}_1}(i)}{\binom{\varphi}{i}} = \frac{\mathcal{C}_{\mathcal{H}_1}(i)}{\binom{\varphi+1}{i}} + \frac{\mathcal{C}_{\mathcal{H}_1}(i+1)}{\binom{\varphi+1}{i+1}}$$

and

$$\frac{\mathcal{C}_{\tilde{\mathcal{G}}_1}(i)}{\binom{\varphi}{i}} = \frac{\mathcal{C}_{\mathcal{G}_1}(i)}{\binom{\varphi+1}{i}} + \frac{\mathcal{C}_{\mathcal{G}_1}(i+1)}{\binom{\varphi+1}{i+1}}.$$

Therefore,

$$\frac{\mathcal{C}_{\mathcal{H}_1}(i)}{\binom{\varphi+1}{i}} + \frac{\mathcal{C}_{\mathcal{H}_1}(i+1)}{\binom{\varphi+1}{i+1}} = \frac{\mathcal{C}_{\mathcal{G}_1}(i)}{\binom{\varphi+1}{i}} + \frac{\mathcal{C}_{\mathcal{G}_1}(i+1)}{\binom{\varphi+1}{i+1}},$$

which implies after some algebraic manipulations and using the induction hypothesis that

$$\Delta_{i+1} = A_{i+1} - B_{i+1} = \mathcal{C}_{\mathcal{H}_1}(i+1) - \mathcal{C}_{\mathcal{G}_1}(i+1) = \frac{\binom{\varphi+1}{i+1}}{\binom{\varphi+1}{i}} \left(\mathcal{C}_{\mathcal{G}_1}(i) - \mathcal{C}_{\mathcal{H}_1}(i)\right)$$

$$= \frac{\binom{\varphi+1}{i+1}}{\binom{\varphi+1}{i}}(B_i - A_i) = \gamma(-1)^{i+1} \binom{\varphi+1}{i+1}$$

□

By Lemma 11 we have that if $\gamma = A_0 - B_0$ then $(\varphi+1)\gamma = B_1 - A_1$, $\binom{\varphi+1}{2}\gamma = A_2 - B_2$ and so on. Without loss of generality we can assume that $\gamma \geq 0$. We will enumerate the difference in the number of vectors from configuration $(0, w)$ which are covered by the first partition compared to the second partition.

Lemma 12. *If $i \leq e$ then a codeword from configuration $(i, w-i)$ e-covers*

$$\sum_{j=0}^{e-i} \binom{w-i}{j} \binom{w+a-\varphi-1+i}{i+j} \tag{14}$$

vectors from configuration $(0, w)$.

Proof. Let $c \in \mathcal{C}$ be a codeword from configuration $(i, w-i)$ and x be a vector from configuration $(0, w)$ such that $d(c, x) \leq e$. c and x differ in i coordinates in the first part of the partition. In the second part of the partition, c can have j positions with ones in which x has zeroes. j must be between 0 and $e-i$ since $d(c, x) \leq e$. Clearly there are exactly $i+j$ position in which x has ones and c has zeroes. The number of combination to choose the j and the $i+j$ positions to obtain a valid vector x is

$$\sum_{j=0}^{e-i} \binom{w-i}{j} \binom{w+a-\varphi-1+i}{i+j}$$

□

Theorem 13. *If $\mathcal{C}$ is an e-perfect code in $J(n, w)$ with strength φ then*

$$\sum_{i=0}^{min(\varphi+1,e)} (-1)^i \binom{\varphi+1}{i} \sum_{j=0}^{e-i} \binom{w-i}{j} \binom{w+a-\varphi-1+i}{i+j} = 0 \tag{15}$$

Proof. The theorem is obtained first by summing Equation (14) on all codewords of $\mathcal{C}$ which e-cover vectors from configuration $(0, w)$ in both partitions, and applying Lemma 11

$$\begin{aligned}
0 = & \sum_{i=0}^{min(\varphi+1,e)} A_i \sum_{j=0}^{e-i} \binom{w-i}{j} \binom{w+a-\varphi-1+i}{i+j} \\
& - \sum_{i=0}^{min(\varphi+1,e)} B_i \sum_{j=0}^{e-i} \binom{w-i}{j} \binom{w+a-\varphi-1+i}{i+j} \\
= & \sum_{i=0}^{min(\varphi+1,e)} \Delta_i \sum_{j=0}^{e-i} \binom{w-i}{j} \binom{w+a-\varphi-1+i}{i+j} \\
= & \sum_{i=0}^{min(\varphi+1,e)} \gamma(-1)^i \binom{\varphi+1}{i} \sum_{j=0}^{e-i} \binom{w-i}{j} \binom{w+a-\varphi-1+i}{i+j}
\end{aligned} \tag{16}$$

Equation (15) is implied by dividing both sides of Equation (16) by γ. Note, that there exist partitions for which $\gamma \neq 0$ as otherwise the strength of the code is at least $\varphi + 1$. □

If $e = 1$ then Equation (15) takes the form

$$1 + w(w + a - \varphi - 1) - (\varphi + 1)(w + a - \varphi) = 0,$$

and the solution for φ is

$$\varphi = \frac{2w + a - 1 - \sqrt{(a+1)^2 + 4(w-1)}}{2}$$

as in Equation (13).

Solutions of Equation (15) for $e = 2$ can be obtained easily. These solutions rules out most possible values. We leave the technical computation to the reader.

5. DISCUSSION AND OPEN PROBLEMS

Our research was motivated by the long standing conjecture of Delsarte that there are no nontrivial perfect codes in the Johnson scheme. Steiner systems, t-designs, and configuration distribution might be the key for proving the conjecture.

A. Three Sets of Parameters

For the solution of the question whether e-perfect codes exists in $J(n, w)$ we believe that we need to distinguish between 3 sets of parameters:

A.1. *1-Perfect Codes*

If one might think that there are e-perfect codes in the Johnson scheme, then $e = 1$ is the first place to search for such codes. There are two reasons:

- In other schemes and models, where perfect codes exist, there are perfect codes with radius 1.
- Equation (15) has a many solutions for radius $e = 1$, while for $e = 2$ not many solutions were found. The equations are becoming more and more complicated and it is tempting to conjecture that there are no integer solutions to the equation for $e > 2$.

A.2. *e-Perfect Codes in J(2w,w)*

The trivial perfect codes (beside a single codeword or the whole space) are in the graph $J(2w, w)$, w odd. Are there more perfect codes in $J(2w, w)$? There are a few properties which are unique for such graph. In [4] it was proved that an e-perfect code $\mathcal{C}$ in $J(2w, w)$ is self complement, that is, $\mathcal{C} = \bar{\mathcal{C}}$. An immediate consequence is that given a partition $\{\mathcal{H}_1, \mathcal{H}_2\}$ of $\mathcal{N}$, such that $|\mathcal{H}_1| = k$ and $|\mathcal{H}_2| = n - k$, then $A_i = A_{k-i}$ for all i. More than that, if the strength of the code is $k - 1$ then for two such partitions with configuration distributions $(A_i)_{i=0}^k$ and $(B_i)_{i=0}^k$ we have $\Delta_i = \Delta_{k-i}$ and hence by Lemma 11 we have that k must be even, or in other words, the strength of the code is odd.

A.3. *e-Perfect Codes, e ≥ 2*

In this case we do not expect to have many integers solutions to Equation (15). Therefore, the main task should be to prove an upper bound on the number of integer solutions for the equation. Such a bound will also be a bound on the number of e-perfect code that exist when $e \geq 2$. The cases which will remain unsolved might be handled with the divisibility conditions of Equation (1).

B. Other Directions

There are few other directions in which the conjecture of Delsarte can be attacked:

B.1. *Improving the Roos Bound*

Theorem 1 introduces an upper bound on n as a function of w and e. An improvement on this bound would not solve any of the three sets of parameters, but it can limit considerably the range in which e-perfect codes can exist in $J(n, w)$. In this context a lower bound on w as a function of e is also of interest as a result of Theorem 3. Some lower bounds on w as function of e were given in [6].

B.2. *More Steiner Systems*

We have enumerated the number of Steiner system known to be embedded in e-perfect code in $J(n, w)$ by Theorem 4. If we can prove that more Steiner systems with new parameters must exist in an e-perfect code then by the necessary conditions of Theorem 2 we might be able to restrict considerably the set of parameters in which e-perfect codes can exist.

B.3. *The Strength of the Code*

The divisibility conditions of Equation (1) are essential in proving that for certain values of e there are no e-perfect codes or only finite number of codes can exist (see Theorem 3). Finding better lower bounds on the strength of a perfect code will produce more divisibilty conditions to be fulfilled in Equation (1). Therefore, the computation of the strength is so important.

B.4. *Configuration Distribution and Moments*

The exact values of the configuration distribution and moments of an e-perfect code might provide an essential information for excluding the existence of e-perfect codes in $J(n, w)$. We believe that this would be most important for $e \geq 2$, where the evaluation of the strength is more difficult (compared to $e = 1$).

Of course, there are other ways to tackle the problems, such as a generalized Lloyd theorem [3] or the connection between t-designs and T-designs [3,8]. The techniques of Martin [9] mentioned earlier could also help. Finally, we hope that the tools used in this article, especially configuration distribution and moments might be of help in examining properties of other codes in the Johnson scheme, that is, constant weight codes.

REFERENCES

[1] E. Bannai, Codes in bi-partite distance-regular graphs, Journal London Math Soc 2 (1977), 197–202.

[2] E. Biggs, Perfect codes in graphs, J Combin Theory, Series B, 15 (1973), 289–296.

[3] P. Delsarte, An algebraic approach to association schemes and coding theory, Philips Journal Res 10 (1973), 1–97.

[4] T. Etzion, On the nonexistence of perfect codes in the Johnson scheme, SIAM J Discrete Math 9 (1996), 201–209.

[5] T. Etzion, On perfect codes in the Johnson scheme, DIMACS Series Discrete Math Theor Comput Sci 56 (2001), 125–130.

[6] T. Etzion and M. Schwartz, Perfect constant-weight codes, IEEE Trans Inf Theory IT-50 (2004), 2156–2165.

[7] P. Hammond, On the non-existence of perfect codes and nearly perfect codes, Discrete Math 39 (1982), 105–109.

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

[9] W. J. Martin, Completely Regular Subsets, Ph.D. Thesis, University of Waterloo, 1992.

[10] V. Pless, Power moment identities on weight distributions in error correcting codes, Inf Control 6 (1963), 147–152.

[11] V. Pless, Introduction to the Theory of Error-Correcting Codes, Wiley, New York, 1990.

[12] C. Roos, A note on the existence of perfect constant weight codes, Discrete Math 47 (1983), 121–123.

[13] Juriaan Simonis, MacWilliams identities and coordinate partitions, Linear Algebra Appl 216 (1995), 81–91.

[14] O. Shimabukuro, On the nonexistence of perfect codes in $J(2w + p^2, w)$, Ars Combinatoria 75 (2005), 129–134.