Perfect Constant-Weight Codes

Tuvi Etzion, *Fellow, IEEE,* and Moshe Schwartz, *Member, IEEE*

***Abstract*—In his pioneering work from 1973, Delsarte conjectured that there are no nontrivial perfect codes in the Johnson scheme. Many attempts were made, during the years which followed, to prove Delsarte's conjecture, but only partial results have been obtained. We survey all these attempts, and prove some new results having the same flavor. We also present a new method, taking a different approach, which we hope can lead to the settling of this conjecture. We show how this new method rules out sets of parameters as well as specific given parameters.**

***Index Terms*—Constant-weight codes, Johnson scheme, k-regular codes, perfect codes, Steiner systems.**

I. Introduction

In a given metric, codes which attain the sphere-packing bound in the metric are called perfect. Such codes have always drawn the attention of coding theorists and mathematicians. In the Hamming scheme, all perfect codes over finite fields are known [1]. They exist for only a relatively small number of parameters, while for other parameters it was proved [1]–[4] that they cannot exist. The nonexistence proof is based of Lloyd's polynomials. For non-field alphabets only trivial codes are known and by similar methods it was proved [5] that for most other parameters they do not exist.

Constant-weight codes are building blocks for general codes in the Hamming scheme. They are also of interest in a wide range of areas [6]–[10]. A natural question is whether there exist perfect constant-weight codes. In the 1970s and 1980s, most work on constant-weight codes considered only the binary case. A binary constant-weight code has three parameters: length n, constant weight w, and minimum Hamming distance $d = 2\delta$ (Hamming distance will be called *H-distance* for short). If we define the distance between two words x and y of weight w, as half their H-distance, we obtain a new metric which is called the Johnson metric, and the distance is called the *J-distance*.

It is very convenient to describe the Johnson scheme in terms of sets. With the Johnson scheme we associate the Johnson graph $J(n, w)$. The vertex set V_w^n of the Johnson graph consists of all w-subsets of a fixed n-set. Two such w-subsets are adjacent if and only if their intersection has size $w-1$. 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 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 J-distance between v and c is at most e. 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 [11], that these are the only perfect codes in $J(n, w)$.

Manuscript received May 1, 2003; revised May 13, 2004. The material in this correspondence was presented in part at the 991st AMS Meeting, University of North Carolina, Chapel Hill, NC, October 2003.

The authors are with the Computer Science Department, Technion–Israel Institute of Technology, 32000 Haifa, Israel (e-mail: etzion@cs.technion.ac.il; moosh@cs.technion.ac.il).

Communicated by C. Carlet, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2004.833355

The main purpose of this correspondence is to present a new technique which could lead to the settling of the existence question of perfect codes in the Johnson scheme. In Section II, we give a short survey of the known results and techniques concerning the existence of perfect codes in the Johnson scheme. Parameters for which perfect codes cannot exist are summarized. In Section III, we present some new results using similar techniques, which rule out more parameters for which perfect codes cannot exist. In Section IV, we present a new technique to prove that e-perfect codes do not exist in $J(n, w)$. We show which general parameters can be ruled out by the new technique. In Section V, we summarize the parameters for which there are no e-perfect codes in $J(n, w)$. We also describe a computer search, using the new technique, with which we were able to show the nonexistence of e-perfect codes in $J(n, w)$ for any given specific e, n, and w that we checked. Conclusion is given in Section VI.

II. Survey of Known Results

In his work from 1973, Delsarte wrote [11, p. 55]:

> "After having recalled that there are "very few" perfect codes in the Hamming schemes, one must say that, for $1 < \delta < n$, there is not a single one known in the Johnson schemes. It is tempting to risk the conjecture that such codes do not exist. Certain results contained in the present work could be useful to attack this problem; especially the generalized Lloyd theorem of sec. 5.2.2 and theorem 4.7 about t-designs."

Indeed, Delsarte omitted the trivial perfect codes (we will omit them too, so when we say perfect codes we mean nontrivial perfect codes) and his conjecture on the nonexistence of perfect codes in the Johnson scheme has provided lots of ground for research in the ten years which followed. Due to the fact that in the Hamming scheme all parameters for which perfect codes exist were known, special emphasis was given to the Johnson scheme. However, most research failed to produce significant results.

In the Hamming scheme, the trivial codes, the Hamming codes, and the two Golay codes, are the only perfect codes over GF(q). There are no perfect codes with other parameters [2]–[4] (see also [1] for the detailed proof). Moreover, for most parameters, it is known that there are no perfect codes over non-field size alphabets in the Hamming scheme [5].

Biggs [12] showed that the natural setting for the existence problem of perfect codes is the class of distance-transitive graphs. Let Γ be a connected graph. We denote by $d_\Gamma(x, y)$ the length of the shortest path from x to y. Γ is said to be *distance-transitive* if, whenever x, x', y, y' are vertices with $d_\Gamma(x, x') = d_\Gamma(y, y')$, there is an automorphism γ of Γ with $\gamma(x) = y$ and $\gamma(x') = y'$. Biggs [12] claims that the class of distance-transitive graphs includes all interesting schemes, such as the Hamming scheme and the Johnson scheme. These graphs are contained in another class of graphs. Γ is said to be *distance-regular* if there are integers a_i, b_i, c_i ($0 \le i \le d$, where d is the diameter of Γ) with the following property: whenever x and x' are vertices with $d_\Gamma(x, x') = i$, then

$$\left|\left\{y : d_\Gamma(x, y) = j \text{ and } d_\Gamma(x', y) = 1\right\}\right| = a_i,\ b_i,\ \text{or } c_i$$

depending on whether $j = i-1, i$, or $i+1$. A distance-transitive graph is obviously distance-regular. Let Γ be a distance-regular graph with a vertex set $\mathcal{V}$. A subset $\mathcal{X}$ of $\mathcal{V}$ is called an *anticode* with diameter δ, if δ is the maximum distance occurring between vertices of $\mathcal{X}$. Anticodes with diameter δ having maximal size are called *optimal anticodes*. The following theorem is due to Delsarte [11].

Theorem 1: Let $\mathcal{X}$ and $\mathcal{Y}$ be subsets of $\mathcal{V}$ such that the nonzero distances occurring between vertices of $\mathcal{X}$ do not occur between vertices of $\mathcal{Y}$. Then $|X| \cdot |\mathcal{Y}| \leq |\mathcal{V}|$.

Biggs [12] developed a general theory and a "simple" criterion for the existence of perfect codes in a distance-transitive graph. He showed that this criterion implies Lloyd's theorem, which is used in the Hamming scheme to prove the nonexistence of perfect codes in all cases. Bannai [13] proved the nonexistence of e-perfect codes in $J(2w-1, w)$ and $J(2w+1, w)$ for $e \geq 2$. He used an analog to Lloyd's theorem and some number-theoretic results. Hammond [14] improved this result by proving the following.

Theorem 2: There are no perfect codes in $J(2w - 2, w)$, $J(2w - 1, w)$, $J(2w + 1, w)$, and $J(2w + 2, w)$.

However, the most significant result, in the first 20 years following Delsarte's conjecture, was given in 1983 by Roos [15].

Theorem 3: If an e-perfect code exists in $J(n, w)$, then

$$n \leq (w - 1)\frac{2e + 1}{e}.$$

The proof of Roos was based on the following theory given by Delsarte [11]: by using Theorem 1, Roos noticed that if an e-perfect code exists, then the e-spheres should be optimal anticodes with diameter $2e$. He proceeded to find anticodes in $J(n, w)$ and obtained his result by comparing them to the e-spheres. In Section III, we will give a different simple proof to Theorem 3. There is a special interest in the technique of Roos and Theorem 1 of Delsarte as we will discuss in Section II-A.

It took more than 10 years to obtain new results. Etzion [16] took a new approach. He proved that if there exists a nontrivial e-perfect code $\mathcal{C}$ in $J(n, w)$, then many Steiner systems are embedded in $\mathcal{C}$. A Steiner system $S(t, k, n)$ is a collection of k-subsets (called *blocks*) taken from an n-set, such that each t-subset of the n-set is contained in exactly one block. The following theorems are well known (see [1] for reference).

Theorem 4: If there exists a Steiner system $S(t, k, n)$ for $t \geq 1$, then there exists a Steiner system $S(t - 1, k - 1, n - 1)$.

Theorem 5: A necessary condition for a Steiner system $S(t, k, n)$ to exist, is that the numbers

$$\binom{n-i}{t-i} \Big/ \binom{k-i}{t-i}$$

must be integers, for all $0 \leq i \leq t$.

Using Etzion's approach, the necessary conditions of Theorem 5 imply necessary conditions for the existence of perfect codes in the Johnson scheme. Moreover, Etzion developed a new concept called *configuration distribution*, which is akin to the concept of weight distribution for codes in the Hamming scheme. Using this concept, combined with the necessary conditions derived from Steiner systems, many parameters were found, for which e-perfect codes do not exist in $J(n, w)$. We summarize the main results given in [16].

Lemma 1: If $\mathcal{C}$ is an e-perfect code in the Johnson scheme, then its minimum H-distance is $4e + 2$.

An (n, d, w) code is a code of length n, constant weight w, and minimum H-distance d. $A(n, d, w)$ denotes the maximum size of an (n, d, w) code. The following lemma is a trivial observation.

Lemma 2: If $\mathcal{C}$ is an e-perfect code in $J(n, w)$, then

$$A(n, 4e + 2, w) = |\mathcal{C}|.$$

Henceforth, let $\mathcal{N} = \{1, 2, \ldots, n\}$ be the n-set. From a Steiner system $S(t, k, n)$ we construct a constant-weight code on n coordinates as follows. From each block $\mathcal{B}$ we construct a codeword with 1's in the positions of $\mathcal{B}$ and 0's in the positions of $\mathcal{N} \setminus \mathcal{B}$. This construction leads to the following well-known theorem (see reference in [7]).

Theorem 6:

$$A(n, 2(k - t + 1), k) = \frac{n(n-1)\cdots(n-t+1)}{k(k-1)\cdots(k-t+1)}$$

if and only if a Steiner system $S(t, k, n)$ exists.

From Theorem 6 and Lemmas 1 and 2, we immediately infer the following result.

Lemma 3: If $\mathcal{C}$ is an e-perfect code in $J(n, w)$ which is also a Steiner system, then it is a Steiner system $S(w - 2e, w, n)$.

The next lemma is a simple observation of a considerable use.

Lemma 4: The complement of an e-perfect code in $J(n, w)$ is an e-perfect code in $J(n, n - w)$.

Finally, we need a few more definitions which we will use in the proofs of the nonexistence theorems in the sequel. For a given partition of $\mathcal{N}$ into two subsets $\mathcal{A}$ and $\mathcal{B}$, such that $|\mathcal{A}| = k$ and $|\mathcal{B}| = n - k$, let *configuration* (i, j) consist of all vectors with weight i in the positions of $\mathcal{A}$ and weight j in the positions of $\mathcal{B}$.

For an e-perfect code $\mathcal{C}$ in $J(n, w)$, we say that $u \in \mathcal{C}$ *J-covers* $v \in V_w^n$ if the J-distance between u and v is at most e. 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 the two different notations. The following results were proved in [16].

Theorem 7: If an e-perfect code exists in $J(n, w)$, then a Steiner system $S(e+1, 2e+1, w)$ and a Steiner system $S(e+1, 2e+1, n-w)$ exist.

Corollary 1: If an e-perfect code exists in $J(n, w)$, then a Steiner system $S(2, e + 2, w - e + 1)$ and a Steiner system $S(2, e + 2, n - w - e + 1)$ exist.

Corollary 2: If an e-perfect code exists in $J(n, w)$, then $n - w \equiv w \equiv e \pmod{e + 1}$ and hence $e + 1$ divides $n - 2w$.

Theorem 8: Except for the Steiner systems $S(1, w, n)$ and $S(w, w, n)$, there are no more Steiner systems which are also perfect codes in the Johnson scheme.

Theorem 9: There are no e-perfect codes in $J(2w + p, w)$, p prime, in $J(2w + 2p, w)$, p prime, $p \neq 3$, and in $J(2w + 3p, w)$, p prime, $p \neq 2, 3, 5$.

If we combine Lemma 4 with the fact that the J-distance between words of an e-perfect code is at least $2e + 1$, we get the following.

Corollary 3: If an e-perfect code exists in $J(n, w)$, then $w \geq 2e+1$ and $n - w \geq 2e + 1$.

To give the reader the flavor of the methods used in [16], we use similar methods to provide a much simpler proof of Theorem 3, and to prove that there are even more Steiner systems embedded in perfect codes in the Johnson scheme (these results were also presented in [17]).

Theorem 10: If an e-perfect code exists in $J(n, w)$ then

$$n \leq (w - 1)\frac{2e + 1}{e}.$$

Proof: Assume $\mathcal{C}$ is an e-perfect code in $J(n,w)$. We partition $\mathcal{N}$ into two subsets $\mathcal{A}$ and $\mathcal{B}$, such that $|\mathcal{A}| = n-w+1, |\mathcal{B}| = w-1$, and there is a codeword of configuration $(e+1, w-e-1)$. Clearly, the J-distance between a vector from configuration $(e+1, w-e-1)$ and a vector from configuration $(e+1-i, w-e-1+i), 0 < i \leq e$, is strictly less than $2e+1$, so $\mathcal{C}$ does not have any codeword from configuration $(e+1-i, w-e-1+i)$. Therefore, all the vectors from configuration $(1, w-1)$ are J-covered by codewords from configuration $(e+1, w-e-1)$. To J-cover each vector from configuration $(1, w-1)$ exactly once we must have exactly $\frac{n-w+1}{e+1}$ codewords from configuration $(e+1, w-e-1)$. Since the minimum J-distance of $\mathcal{C}$ is $2e+1$, two codewords from configuration $(e+1, w-e-1)$ cannot intersect in the zeroes of part $\mathcal{B}$. Hence, $w-1 \geq \frac{n-w+1}{e+1}e$, which is equivalent to $n \leq (w-1)\frac{2e+1}{e}$. □

Theorem 11: If an e-perfect code exists in $J(n,w)$ and $n < (w-1)(2e+1)/e$, then an $S(2, e+2, n-w+2)$ exists.

Proof: Assume $\mathcal{C}$ is an e-perfect code in $J(n,w)$. As in the proof of Theorem 11, we partition $\mathcal{N}$ into two subsets $\mathcal{A}$ and $\mathcal{B}$, such that $|\mathcal{A}| = n-w+1, |\mathcal{B}| = w-1$, and there are $\frac{n-w+1}{e+1}$ codewords from configuration $(e+1, w-e-1)$. Since $n < (w-1)(2e+1)/e$, i.e., $\frac{n-w+1}{e+1}e < w-1$, we have at least one coordinate in $\mathcal{B}$ which has ones in all the codewords from configuration $(e+1, w-e-1)$. We remove this coordinate from $\mathcal{B}$ to obtain $\mathcal{B}_1$ and join it to $\mathcal{A}$ to obtain $\mathcal{A}_1$. $|\mathcal{A}_1| = n-w+2$, $|\mathcal{B}_1| = w-2$, and $\mathcal{C}$ does not have any codeword from configuration $(e+2-i, w-e-2+i)$, $i > 0$. Therefore, all the vectors from configuration $(2, w-2)$ are J-covered by codewords from configuration $(e+2, w-e-2)$. Since each vector from configuration $(2, w-2)$ must be J-covered by exactly one codeword from configuration $(e+2, w-e-2)$, it follows that part $\mathcal{A}_1$ of the codewords from configuration $(e+2, w-e-2)$ forms a Steiner system $S(2, e+2, n-w+2)$. □

Corollary 4: If an e-perfect code exists in $J(2w+a, w)$, $a \geq 0$, then an $S(2, e+2, w+2)$ exists.

Martin also examined the existence problem when he considered completely regular subsets in his Ph.D. dissertation [18]. He found that if $e = 1$, then perfect codes must obey some numerical formulas. Etzion [17] polished some of the results from [16].

Recently, Shimabukuro [19] showed that, as an application of Etzion's results, one can obtain that there are no perfect codes in

- $J(2w+5p, w)$, p prime, $p \neq 3$;
- $J(2w+p^2, w)$, p prime.

A. Steiner Systems and Perfect Codes

Steiner systems play an important role in ruling out the existence of e-perfect codes in $J(n,w)$. Moreover, the Steiner systems $S(1, w, 2w)$, w odd, and $S(w, w, n)$, are among the trivial perfect codes in the Johnson scheme. Theorem 8 states that there are no more Steiner systems which are also perfect codes in the Johnson scheme. By Theorem 6, any Steiner system is an optimal constant-weight code. Obviously, any e-perfect code in $J(n,w)$ is also an optimal constant-weight code. Since in a Steiner system $S(t,k,n)$ each t-subset appears in exactly one block, it would be natural to think that Steiner systems are perfect codes of some kind.

By Lemma 2, an e-perfect code in $J(n,w)$ is an optimal $(n, 4e+2, w)$ code and the size of such a code is clearly

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

By Theorem 6, a Steiner system $S(w-2e, w, n)$ is an optimal $(n, 4e+2, w)$ code and its size is

$$s(n,w,e) = \frac{n!(2e)!}{(n-w+2e)!w!}.$$

If $j(n,w,e) > s(n,w,e)$ then there is no e-perfect code in $J(n,w)$ and if $s(n,w,e) > j(n,w,e)$ then there is no Steiner system $S(w-2e, w, n)$. Note that $j(n,w,e) = s(n,w,e)$ when $n = 2w = 4e+2$ in which case a trivial Steiner system $S(1, 2e+1, 4e+2)$ and a trivial e-perfect code in $J(4e+2, 2e+1)$ exist. No new bounds for either e-perfect codes in $J(n,w)$ or Steiner systems $S(w-2e, w, n)$ can be derived from these conditions.

Recently, Ahlswede, Aydinian, and Khachatrian [20] gave a new interesting definition of diameter-perfect codes (D-perfect codes). They examined a variant of Theorem 1. Let Γ be a distance-regular graph with a vertex set $\mathcal{V}$. If $\mathcal{A}$ is an anticode in Γ, denote by $D(\mathcal{A})$ the diameter of $\mathcal{A}$. Now let

$$\mathcal{A}^*(D) = \max\{|\mathcal{A}| : D(\mathcal{A}) \leq D\}.$$

Theorem 12: If $\mathcal{C}$ is a code in Γ with minimum distance $D+1$, then $|\mathcal{C}| \leq |\mathcal{V}|\,\mathcal{A}^*(D)^{-1}$.

They continued with the following new definition for perfect codes. A code $\mathcal{C}$ with minimum distance $D+1$ is called D-perfect if Theorem 12 holds with equality. This is a generalization of the usual definition of e-perfect codes as e-spheres are anticodes with diameter $2e$.

This new definition for perfect codes introduced some new classes of perfect codes. The interesting classes are those of codes which attain some classical bound. In the Johnson scheme, it was proved that all Steiner systems are D-perfect, thus showing more connections between Steiner systems and perfect codes.

III. New Results

In this section, we continue to prove results on the structure of e-perfect codes in $J(n,w)$. As a result, we identify more parameters of e, n, and w, in which such codes cannot exist.

A. New Upper Bound on n

We first show that no nontrivial e-perfect code achieves Roos' bound with equality. This seemingly slight improvement has many applications.

Theorem 13: If there exists an e-perfect code in $J(n,w)$ then

$$n < (w-1)\frac{2e+1}{e}.$$

Proof: If $n < 2w$ then by Corollary 3 the claim is obvious. Assume $\mathcal{C}$ is an e-perfect code in $J(n,w)$, where $n = 2w+a$, $a \geq 0$, and $n = (w-1)\frac{2e+1}{e}$. If $a = 0$, then $n = 2w$ and $n = (w-1)\frac{2e+1}{e}$ imply that $w = 2e+1$, i.e., $\mathcal{C}$ is a trivial perfect code. By Theorem 2, we have that there are no perfect codes in $J(2w+1, w)$, and, therefore, $a \geq 2$.

Let $b = e+1$; by Corollary 2, $a = n-2w \equiv 0 \pmod b$, and hence, $2 \leq b \leq a$. We substitute $b = e+1$ and $n = 2w+a$, in $n = (w-1)\frac{2e+1}{e}$, and obtain $w = ab-a+2b-1$. By previous theorems, the following Steiner systems must exist.

- By Corollary 1, there exists a Steiner system $S(2, b+1, ab-a+b+1)$. Thus, by Theorem 5, $\frac{\binom{ab-a+b+1}{2}}{\binom{b+1}{2}}$ must be an integer.
- By Corollary 1 there also exists a Steiner system $S(2, b+1, ab+b+1)$. Thus, by Theorem 5, $\frac{\binom{ab+b+1}{2}}{\binom{b+1}{2}}$ must be an integer.

- By Corollary 4, there also exists a Steiner system $S(2, b+1, ab-a+2b+1)$. Thus, by Theorem 5, $\frac{\binom{ab-a+2b+1}{2}}{\binom{b+1}{2}}$ must be an integer.

Therefore,

$$\frac{\binom{ab+b+1}{2}}{\binom{b+1}{2}} - \frac{\binom{ab-a+b+1}{2}}{\binom{b+1}{2}} = \frac{2a^2 - a^2/b + 2a + a/b}{b+1}$$

is an integer, and hence,

$$2a^2 - a^2/b + 2a + a/b \equiv 0 \pmod{b+1}.$$

But, since $b \equiv -1 \pmod{b+1}$, we have that

$$3a^2 + a \equiv 0 \pmod{b+1}. \tag{1}$$

We also have that

$$\frac{\binom{ab-a+2b+1}{2}}{\binom{b+1}{2}} - \frac{\binom{ab-a+b+1}{2}}{\binom{b+1}{2}} = \frac{2ab - 2a + 3b + 1}{b+1}$$

is an integer, and hence,

$$2ab - 2a + 3b + 1 \equiv 0 \pmod{b+1}.$$

Again, $b \equiv -1 \pmod{b+1}$ which implies that

$$4a + 2 \equiv 0 \pmod{b+1}. \tag{2}$$

By (1) and (2) we have that

$$8(3a^2 + a) - (6a-1)(4a+2) \equiv 0 \pmod{b+1}. \tag{3}$$

But, $8(3a^2+a)-(6a-1)(4a+2) = 2$ and clearly 2 is not divisible by $b+1$, a contradiction. Hence, $n < (w-1)\frac{2e+1}{e}$. □

By combining Theorem 11, Corollary 4, and Theorem 13 we conclude as follows.

Corollary 5: If an e-perfect code exists in $J(n, w)$, then a Steiner system $S(2, e+2, w+2)$ and a Steiner system $S(2, e+2, n-w+2)$ exist.

B. Applications

Lemma 4 implies that it is sufficient to prove that there are no e-perfect codes in $J(n, w)$ for $n \geq 2w$. Therefore, in the sequel, we assume that $w \leq n - w$. Assume that an e-perfect code exists in $J(n, w)$. By Corollaries 1 and 5, the following Steiner systems must exist:

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

By Theorem 5, we have that

- $(e+1)(e+2)$ divides $(w+1)(w+2)$.
- $(e+1)(e+2)$ divides $(n-w+1)(n-w+2)$.
- $(e+1)(e+2)$ divides $(w-e)(w-e+1)$.
- $(e+1)(e+2)$ divides $(n-w-e)(n-w-e+1)$.

Since $(n-w+1)(n-w+2) - (w+1)(w+2) = (n+3)(n-2w)$ it follows that

$$(e+1)(e+2) \text{ divides } (n+3)(n-2w). \tag{4}$$

Since $(n-w-e)(n-w-e+1) - (w-e)(w-e+1) = (n-2e+1)(n-2w)$ it follows that

$$(e+1)(e+2) \text{ divides } (n-2e+1)(n-2w). \tag{5}$$

By Corollary 2, we have that $e+1$ divides $n-2w$ and, therefore, by (5) we have

$$(e+1)(e+2) \text{ divides } (n+5)(n-2w). \tag{6}$$

Thus, from (4) and(6) we have

$$(e+1)(e+2) \text{ divides } 2(n-2w). \tag{7}$$

Therefore, by Corollary 2, (4), and(7), we obtain the following theorem.

Theorem 14: 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 $e \equiv 0 \pmod 4$ and $(e+1)(e+2)/2$ divides $n-2w$.

Corollary 6: Assume there exists an e-perfect code in $J(n, w)$.

- If n is even then $(e+1)(e+2)$ divides $n-2w$.
- If n is odd then $e \equiv 0 \pmod 4$ and $(e+1)(e+2)/2$ divides $n-2w$.

Corollary 7: 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 $p \neq 2q-1$.

C. A Lower Bound on w

In this subsection, we give a lower bound on w if there exists an e-perfect code $\mathcal{C}$ in $J(n, w)$. This bound will be used in our application of the main result in Section IV. We assume the existence of an e-perfect code in $J(n, w)$ and as usual $w \leq n - w$.

Theorem 15: If there exists an e-perfect code in $J(n, w)$, $w < n-w$, then

$$w > \frac{e(e+1)(e+2)}{2} + 2e + 1$$

if n is odd, and $w > e(e+1)(e+2) + 2e + 1$ if n is even.

Proof: We prove the case of n odd. The case of n even is proved similarly. By Corollary 6, we have that $\frac{(e+1)(e+2)}{2}$ divides $n-2w$ and, hence,

$$\frac{(e+1)(e+2)}{2} \leq n - 2w.$$

By Theorem 13, we have that $n - 2w < \frac{w-2e-1}{e}$ and hence $\frac{(e+1)(e+2)}{2} < \frac{w-2e-1}{e}$. Thus,

$$w > \frac{e(e+1)(e+2)}{2} + 2e + 1. \qquad \square$$

We now handle the case of $n = 2w$. We denote $w = 2e+1+\varepsilon$ and $n = 4e+2+2\varepsilon$, where $\varepsilon \geq 0$ by Corollary 3. We partition the set of coordinates $\mathcal{N}$ into two subsets $\mathcal{A}$ and $\mathcal{B}$, such that $|\mathcal{A}| = |\mathcal{B}| = w$, and there is a codeword from configuration $(w, 0)$. Let $\mathcal{C}(i)$ denote the number of codewords with i ones in the positions of $\mathcal{A}$. Now, one can easily verify (see also [16]) that

$$\mathcal{C}(w-2e-1) = \left[\frac{(2e+1+\varepsilon)!e!}{(2e+1)!(e+\varepsilon)!}\right]^2$$
$$\mathcal{C}(w-2e-2) = \mathcal{C}(w-2e-1)\frac{1}{(2e+2)^2}(\varepsilon^2 - 2e(e+1)\varepsilon).$$

Since $\mathcal{C}(w-2e-2)$ is obviously nonnegative, we have

$$\varepsilon^2 \geq 2e(e+1)\varepsilon.$$

We note that $\varepsilon > 0$ or else the code is trivial. Then

$$\varepsilon \geq 2e(e+1).$$

Therefore, we have the following.

Theorem 16: If an e-perfect code exists in $J(n, w)$, $n = 2w$, then

$$w \geq 2e^2 + 4e + 1.$$

IV. k-Regular Codes

In this section, we present a new approach to rule out the existence of e-perfect codes in $J(n,w)$. We note that all the known divisibility conditions which rule out perfect codes are derived from Steiner systems. In this section, we investigate the divisibility conditions which are derived from the size of the code as given by the sphere-packing bound. In $J(n,w)$, let us denote

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

the size of a sphere of radius e. The number of codewords of an e-perfect code $\mathcal{C}$ in $J(n,w)$ is

$$|\mathcal{C}|=\frac{\binom{n}{w}}{\Phi_e(n,w)}$$

by the sphere-packing bound, and hence we have that

$$\Phi_e(n,w)\left|\binom{n}{w}\right.. \tag{8}$$

However, we may do much better than this by introducing the notion of k-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 $\mathcal{N}=\{1,\ldots,n\}$. For all $0\le i\le|\mathcal{A}|$ we define

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

Also, for each $I\subseteq\mathcal{A}$ 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 *k-regular*, if the following two conditions hold.

(c.1) There exist numbers $\alpha(0),\ldots,\alpha(k)$ such that if $\mathcal{A}\subseteq\mathcal{N}$, $|\mathcal{A}|=k$, then $\mathcal{C}_{\mathcal{A}}(i)=\alpha(i)$ for all $0\le i\le k$.

(c.2) For any given k-subset $\mathcal{A}$ of $\mathcal{N}$, there exist numbers $\beta_{\mathcal{A}}(0),\ldots,\beta_{\mathcal{A}}(k)$ such that if $I\subseteq\mathcal{A}$ then $\mathcal{C}_{\mathcal{A}}(I)=\beta_{\mathcal{A}}(|I|)$.

Note that if a code is k-regular, $k\ge1$, then it is also $(k-1)$-regular. Now, (8) is a simple result of the following theorem and the fact that all codes are trivially 0-regular.

Theorem 17: If an e-perfect code $\mathcal{C}$ in $J(n,w)$ is k-regular, then

$$\Phi_e(n,w)\ \left|\ \binom{n-i}{w-i}\right.$$

for all $0\le i\le k$.

Proof: Let $\mathcal{C}$ be an e-perfect code in $J(n,w)$ which is k-regular. Let $0\le i\le k$, and by condition (c.1), let χ denote the number of length i all-ones words appearing in a projection of $\mathcal{C}$ onto i coordinates. We may, therefore, write the following equation, which counts in two different ways the total number of length i all-ones words appearing in all the projections of $\mathcal{C}$ onto i coordinates:

$$\frac{\binom{n}{w}}{\Phi_e(n,w)}\binom{w}{i}=\binom{n}{i}\chi.$$

Therefore,

$$\chi=\frac{\binom{n-i}{w-i}}{\Phi_e(n,w)}$$

for each i, $0\le i\le k$. □

For the rest of our discussion, we examine e-perfect codes in $J(2w+a,w)$. We define the following polynomial which plays a crucial role:

$$\sigma_e(w,a,k)\triangleq\sum_{j=0}^{e}(-1)^j\binom{k}{j}\sum_{i=0}^{e-j}\binom{w-j}{i}\binom{w+a-k+j}{i+j}.$$

Theorem 18: Let $\mathcal{C}$ be an e-perfect code in $J(2w+a,w)$, and let $1\le k\le w$. If $\sigma_e(w,a,m)\ne0$ for all the integers $1\le m\le k$, then $\mathcal{C}$ is k-regular.

Proof: We prove the theorem by induction on k. Let $\mathcal{C}$ be an e-perfect code in $J(2w+a,w)$. We partition the coordinate set into two subsets $\mathcal{A}$ and $\mathcal{B}$, such that $|\mathcal{A}|=k$ and $|\mathcal{B}|=2w+a-k$.

The basis for the induction is $k=1$. We obtain the following two equations:

$$\mathcal{C}_{\mathcal{A}}(0)\sum_{i=0}^{e}\binom{w}{i}\binom{w+a-1}{i}+\mathcal{C}_{\mathcal{A}}(1)\sum_{i=0}^{e-1}\binom{w-1}{i}\binom{w+a}{i+1}=\binom{2w+a-1}{w}$$

$$\mathcal{C}_{\mathcal{A}}(0)+\mathcal{C}_{\mathcal{A}}(1)=\frac{\binom{2w+a}{w}}{\Phi_e(2w+a,w)}.$$

The first equation describes the way codewords of configuration $(0,w)$ and $(1,w-1)$ J-cover words of configuration $(0,w)$. The second equation simply relates $\mathcal{C}_{\mathcal{A}}(0)$ and $\mathcal{C}_{\mathcal{A}}(1)$ to the total number of codewords. To see that this equation set has exactly one solution we have to show that the determinant

$$\begin{vmatrix}\sum_{i=0}^{e}\binom{w}{i}\binom{w+a-1}{i} & \sum_{i=0}^{e-1}\binom{w-1}{i}\binom{w+a}{i+1}\\ 1 & 1\end{vmatrix} \tag{9}$$

is nonzero. But the determinant is simply $\sigma_e(w,a,1)$ which is nonzero by the conditions of the theorem. Since our solution does not depend on the partition, we see immediately that the conditions of Definition 2 are satisfied. Therefore the basis is proved.

Now, for the induction hypothesis, assume that $\mathcal{C}$ is $(k-1)$-regular. Hence, there exist numbers $\alpha'(0),\ldots,\alpha'(k-1)$, such that for each $(k-1)$-subset $\mathcal{A}'$ of $\mathcal{N}$, we have $\mathcal{C}_{\mathcal{A}'}(i)=\alpha'(i)$, for all $0\le i\le k-1$. We now prove the induction step, i.e., that $\mathcal{C}$ is also k-regular. Again, let $\mathcal{A}$ and $\mathcal{B}$ be a partition of the coordinate set $\mathcal{N}$ into two subsets, with $|\mathcal{A}|=k$ and $|\mathcal{B}|=2w+a-k$. We start by showing that condition (c.2) in Definition 2 for regularity is satisfied. This is done by induction on the weight of the $\mathcal{A}$ part. For weight 0 the claim is obvious. Now assume the claim holds for weight i, i.e., each of the length k weight i words appears in the $\mathcal{A}$ part of the codewords the same number of times. We prove that the claim holds for weight $i+1$.

Let $\mathcal{A}'\subseteq\mathcal{A}$, $|\mathcal{A}'|=k-1$, and $\mathcal{B}'\supseteq\mathcal{B}$, $|\mathcal{B}'|=2w+a-k+1$, be a partition of the coordinates which is obtained from $\mathcal{A}$ and $\mathcal{B}$ by moving one coordinate η from $\mathcal{A}$ to $\mathcal{B}$. With these two partitions, fix a length $k-1$ weight i word ω in the $\mathcal{A}'$ part. The number of codewords having this word in their $\mathcal{A}'$ part is given by $\alpha'(i)/\binom{k-1}{i}$ since the code is $(k-1)$-regular. By our last induction assumption concerning weight i, the number of codewords containing ω in the $\mathcal{A}'$ part and a "0" in coordinate η is given by $\mathcal{C}_{\mathcal{A}}(i)/\binom{k}{i}$. Hence, the number of codewords containing ω in their $\mathcal{A}'$ part and a "1" in coordinate η is the difference

$$\frac{\alpha'(i)}{\binom{k-1}{i}}-\frac{\mathcal{C}_{\mathcal{A}}(i)}{\binom{k}{i}}.$$

We now note that the choice of coordinate η has no bearing on the last arguments, i.e., we can use any coordinate of $\mathcal{A}'$ instead of η. Therefore, the number of codewords containing a given weight $i+1$ word in the $\mathcal{A}$ part is $\mathcal{C}_{\mathcal{A}}(i+1)/\binom{k}{i+1}$. Hence, condition (c.2) for regularity is satisfied. Again, note that (c.2) may hold while (c.1) is not satisfied. In fact, we have proved that if (c.1) and (c.2) hold for k, then (c.2) also holds for $k+1$. Therefore, we have k equations in $k+1$ variables

$$\frac{\mathcal{C}_{\mathcal{A}}(i)}{\binom{k}{i}}+\frac{\mathcal{C}_{\mathcal{A}}(i+1)}{\binom{k}{i+1}}=\frac{\alpha'(i)}{\binom{k-1}{i}},\qquad\text{for all } 0\le i\le k-1. \tag{10}$$

Just like in the induction basis, in order to prove condition (c.1) for regularity we add the following equation:

$$\sum_{j=0}^{\min(k,e)} \mathcal{C}_{\mathcal{A}}(j) \sum_{i=0}^{e-j} \binom{w-j}{i} \binom{w+a-k+j}{i+j} = \binom{2w+a-k}{w}. \tag{11}$$

This set of equations has exactly one solution if and only if its determinant is nonzero. This determinant is easily seen to be equal to

$$\prod_{i=0}^{k-1} \frac{1}{\binom{k}{i}} \cdot \left[\sum_{j=0}^{e} (-1)^j \binom{k}{j} \sum_{i=0}^{e-j} \binom{w-j}{i} \binom{w+a-k+j}{i+j} \right] = \prod_{i=0}^{k-1} \frac{1}{\binom{k}{i}} \sigma_e(w,a,k).$$

By our assumption on σ_e, we have a unique solution to the set of (10)–(11). Since the partition does not affect the above arguments, condition (c.1) for regularity holds and $\mathcal{C}$ is k-regular. □

A. 1-Perfect Codes

We now focus on 1-perfect codes and show that they are k-regular for a relatively wide range of values of k.

Theorem 19: If a 1-perfect code exists in $J(2w+a,w)$, then it is k-regular for all

$$0 \le k < \frac{2w+a+1-\sqrt{(a+1)^2+4(w-1)}}{2}.$$

Proof: According to Theorem 18, a 1-perfect code is k-regular in $J(2w+a,w)$ when

$$\sigma_1(w,a,k) = k^2 - (2w+a+1)k + w(w+a) + 1$$

has no integer roots in $[1,k]$. Considered as a polynomial in k, the smaller of the two possible roots is $\frac{2w+a+1-\sqrt{(a+1)^2+4(w-1)}}{2}$, so the range of k described in the theorem contains no integer roots. □

Corollary 8: If a 1-perfect code exists in $J(n,w)$, $n = 2w+a$, then

$$\Phi_1(n,w) = 1 + w(n-w) \;\Big|\; \binom{n-i}{w-i}$$

for all $0 \le i < \frac{2w+a+1-\sqrt{(a+1)^2+4(w-1)}}{2}$.

The following theorem on binomial coefficients will be used to determine nondivisibility of binomial coefficients by powers of primes. The theorem was given by Kummer, and it can be found in [21, p.245].

Theorem 20: Let p be a prime. The number of times p appears in the factorization of $\binom{a}{b}$ equals the number of carries when adding b to $a-b$ in base p.

By [16], we already know that for 1-perfect codes, $w \equiv n-w \equiv 1 \pmod 6$. Hence, $\Phi_1(n,w) \equiv 0 \pmod 2$. We give a stronger result in the following theorem.

Theorem 21: There are no 1-perfect codes in $J(n,w)$, when

$$\Phi_1(n,w) = 1 + w(n-w) \equiv 0 \pmod 4.$$

Proof: Assume there exists a 1-perfect code in $J(n,w)$, $n = 2w+a$ for $2^m \le n \le 2^{m+1}-1$. We have the following two cases.

Case 1: $2^{m-1} \le w \le n/2$. In this case

$$w - 2^{m-1} \le \frac{w}{2} < \frac{2w+a+1-\sqrt{(a+1)^2+4(w-1)}}{2},$$

so by Corollary 8

$$1 + w(n-w) \;\Big|\; \binom{n-w+2^{m-1}}{2^{m-1}}.$$

Theorem 20 implies that

$$\binom{n-w+2^{m-1}}{2^{m-1}} \not\equiv 0 \pmod 4$$

and so

$$1 + w(n-w) \not\equiv 0 \pmod 4.$$

Case 2: $w \le 2^{m-1}-1$. Note that according to Theorem 13, we also have $a < w-3$. If we want to use Corollary 8, we have to show that

$$n - (2^m - 1) < \frac{2w+a+1-\sqrt{(a+1)^2+4(w-1)}}{2} \tag{12}$$

but, after rearranging, this is equivalent to showing that

$$2w + a + \sqrt{(a+1)^2+4(w-1)} < 2^{m+1} - 1.$$

We now notice the following:

$$\begin{aligned} &2w + a + \sqrt{(a+1)^2+4(w-1)} \\ &\quad < 3w - 3 + \sqrt{(w-2)^2+4(w-1)} \text{ since } a < w-3 \\ &\quad = 4w - 3 \le 2^{m+1} - 7 \text{ since } w \le 2^{m-1}-1 \\ &\quad < 2^{m+1} - 1 \end{aligned}$$

as we wanted to show. Hence, (12) holds, and then by Corollary 8

$$1 + w(n-w) \;\Big|\; \binom{2^m-1}{w-n+2^m-1}.$$

Theorem 20 implies that

$$\binom{2^m-1}{w-n+2^m-1} \not\equiv 0 \pmod 4$$

and so

$$1 + w(n-w) \not\equiv 0 \pmod 4.$$ □

Corollary 9: If there exists a 1-perfect code in $J(n,w)$ then either $w \equiv n-w \equiv 1 \pmod{12}$ or $w \equiv n-w \equiv 7 \pmod{12}$.

B. e-Perfect Codes, $e \ge 2$

In this subsection, we discuss nontrivial e-perfect codes when $e \ge 2$. As in Section IV-A, we show that if such a code exists, it must be k-regular for a wide range of values of k.

Theorem 22: If an e-perfect code, $e \ge 2$, exists in $J(2w+a,w)$, then it is k-regular for all $0 \le k < \frac{w}{e} - e$.

Proof: Our aim is to show that $\sigma_e(w,a,k) \ne 0$ for all $k \in [1, w/e-e)$ for the required range of parameters (w, a, and k). We actually show a stronger claim. We show that σ_e is strictly positive in the required range of parameters. We start by noting that the polynomial may be rewritten in the following manner by summing in a different order:

$$\sigma_e(w,a,k) = \sum_{i=0}^{e} \sum_{j=0}^{\min(i,k)} (-1)^j \binom{k}{j} \binom{w-j}{i-j} \binom{w+a-k+j}{i}.$$

We continue and show that in the inner sum, each of the positive summands is greater than its following negative summand in absolute value. This is equivalent to showing that

$$\frac{\binom{k}{j+1}\binom{w-j-1}{i-j-1}\binom{w+a-k+j+1}{i}}{\binom{k}{j}\binom{w-j}{i-j}\binom{w+a-k+j}{i}} < 1.$$

Since $j \geq 0$, $i \leq e$, $a \geq 0$, and $k < w/e - e$

$$\begin{aligned}\frac{\binom{k}{j+1}\binom{w-j-1}{i-j-1}\binom{w+a-k+j+1}{i}}{\binom{k}{j}\binom{w-j}{i-j}\binom{w+a-k+j}{i}} &= \frac{(k-j)(i-j)(w+a-k+j+1)}{(j+1)(w-j)(w+a-k+j+1-i)} \\ &< \frac{(w-e^2)(we-w+e^2+e)}{w(we-w+e)}.\end{aligned}$$

So it suffices to show that

$$\frac{(w-e^2)(we-w+e^2+e)}{w(we-w+e)} \leq 1,$$

but this is equivalent to

$$w(e-2)+e(e+1) \geq 0$$

which always holds. □

Corollary 10: If an e-perfect code exists in $J(n,w)$, then it is e-regular.

Proof: Assume there exists an e-perfect code in $J(n,w)$ By Theorems 15 and 16, we have that $w > 2e^2$ and by Theorem 22 such a code is k-regular for all $k < \frac{w}{e} - e$, and hence the code is e-regular. □

In the next theorem we extend the range of regularity given in Theorem 22. We use Corollary 10 as the starting point for the proof. The method used in the proof of Theorem 22 no longer works for the extended range, so an asymptotic approach is used. We start by giving two simple well-known identities, which can be proved by basic combinatorial techniques.

Lemma 5:

$$\binom{n-p}{m} = \sum_{k=0}^{p}(-1)^k \binom{n-k}{m-k}\binom{p}{k}.$$

Lemma 6: Vandermonde's convolution

$$\binom{n}{m} = \sum_{k=0}^{p}\binom{n-p}{m-k}\binom{p}{k}.$$

Theorem 23: For all $e \geq 2$, there exists $W_e > 0$ such that for all $w \geq W_e$, all e-perfect codes in $J(2w+a,w)$ are $\lfloor \frac{w}{2} \rfloor$-regular.

Proof: Our proof starts essentially the same as the proof of Theorem 22. We actually want to show, that for a large enough w, with $a \geq 0$ and $k \leq w/2$

$$\begin{aligned}\sigma_e(w,a,k) &= \sum_{i=0}^{e}\sum_{j=0}^{\min(i,k)}(-1)^j \binom{k}{j}\binom{w-j}{i-j}\binom{w+a-k+j}{i} \\ &> 0.\end{aligned}$$

By Corollary 10, we may consider $k \geq e$, so we have to show that

$$\sum_{i=0}^{e}\sum_{j=0}^{i}(-1)^j \binom{k}{j}\binom{w-j}{i-j}\binom{w+a-k+j}{i} > 0.$$

The left-hand side can be rewritten as

$$\sum_{i=0}^{e}\frac{\binom{w}{i}}{\binom{w}{k}}\binom{w+a-k}{i}\sum_{j=0}^{i}(-1)^j \binom{i}{j}\binom{w-j}{k-j}\frac{\binom{w+a-k+j}{i}}{\binom{w+a-k}{i}}.$$

We continue by proving that for all $0 \leq i \leq e$, the inner sum is positive, i.e.,

$$\sum_{j=0}^{i}(-1)^j \binom{i}{j}\binom{w-j}{k-j}\frac{\binom{w+a-k+j}{i}}{\binom{w+a-k}{i}} > 0.$$

Now

$$\begin{aligned}\sum_{j=0}^{i}(-1)^j \binom{i}{j}\binom{w-j}{k-j}\frac{\binom{w+a-k+j}{i}}{\binom{w+a-k}{i}} &\geq \sum_{\substack{j=0\\ j\ \text{even}}}^{i}\binom{i}{j}\binom{w-j}{k-j} - \frac{\binom{w+a-k+i}{i}}{\binom{w+a-k}{i}}\sum_{\substack{j=0\\ j\ \text{odd}}}^{i}\binom{i}{j}\binom{w-j}{k-j} \\ &= \sum_{j=0}^{i}(-1)^j \binom{i}{j}\binom{w-j}{k-j} \\ &\quad - \left(\frac{\binom{w+a-k+i}{i}}{\binom{w+a-k}{i}} - 1\right)\sum_{\substack{j=0\\ j\ \text{odd}}}^{i}\binom{i}{j}\binom{w-j}{k-j} \\ &= \binom{w-i}{k} - \left(\frac{\binom{w+a-k+i}{i}}{\binom{w+a-k}{i}} - 1\right)\sum_{\substack{j=0\\ j\ \text{odd}}}^{i}\binom{i}{j}\binom{w-j}{k-j}\end{aligned}$$

where the last step is taken by using Lemma 5. So now it is enough to prove that

$$\left(\frac{\binom{w+a-k+i}{i}}{\binom{w+a-k}{i}} - 1\right)\sum_{\substack{j=0\\ j\ \text{odd}}}^{i}\binom{i}{j}\binom{w-j}{k-j} < \binom{w-i}{k}. \quad (13)$$

We note that the sum may be rewritten in the following manner:

$$\begin{aligned}\sum_{\substack{j=0\\ j\ \text{odd}}}^{i}\binom{i}{j}\binom{w-j}{k-j} &= \frac{1}{2}\left(\sum_{j=0}^{i}\binom{i}{j}\binom{w-j}{k-j} - \sum_{j=0}^{i}(-1)^j \binom{i}{j}\binom{w-j}{k-j}\right) \\ &= \frac{1}{2}\left(\sum_{j=0}^{i}\binom{i}{j}\binom{w-j}{k-j} - \binom{w-i}{k}\right) \quad \text{by Lemma 5.}\end{aligned}$$

Plugging this into (13) we have to prove that,

$$\left(\frac{\binom{w+a-k+i}{i}}{\binom{w+a-k}{i}} - 1\right)\left(\frac{1}{\binom{w-i}{k}}\sum_{j=0}^{i}\binom{i}{j}\binom{w-j}{k-j} - 1\right) < 2. \quad (14)$$

Finally, we have the following chain of inequalities:

$$\begin{aligned}&\left(\frac{\binom{w+a-k+i}{i}}{\binom{w+a-k}{i}} - 1\right)\left(\frac{1}{\binom{w-i}{k}}\sum_{j=0}^{i}\binom{i}{j}\binom{w-j}{k-j} - 1\right) \\ &\quad \leq \left(\left(\frac{w+a-k+1}{w+a-k-i+1}\right)^i - 1\right) \\ &\qquad \cdot \left(\frac{1}{\binom{w-i}{k}}\sum_{j=0}^{i}\binom{i}{j}\binom{w-j}{k-j} - 1\right) \quad (15) \\ &\quad = \left(\left(\frac{w+a-k+1}{w+a-k-i+1}\right)^i - 1\right) \\ &\qquad \cdot \left(\sum_{j=0}^{i}\binom{i}{j}\sum_{\ell=0}^{i-j}\binom{i-j}{\ell}\frac{\binom{w-i}{k-j-\ell}}{\binom{w-i}{k}} - 1\right) \quad (16) \\ &\quad \leq \left(\left(\frac{w+a-k+1}{w+a-k-i+1}\right)^i - 1\right) \\ &\qquad \cdot \left(\sum_{j=0}^{i}\binom{i}{j}\sum_{\ell=0}^{i-j}\binom{i-j}{\ell}\left(\frac{k}{w-i-k+1}\right)^{j+\ell} - 1\right) \quad (17)\end{aligned}$$

$$= \left(\left(\frac{w+a-k+1}{w+a-k-i+1}\right)^i - 1\right) \cdot \left(\sum_{j=0}^{i}\binom{i}{j}\left(\frac{k}{w-i-k+1}\right)^j\left(\frac{w-i+1}{w-i-k+1}\right)^{i-j} - 1\right)$$

$$= \left(\left(\frac{w+a-k+1}{w+a-k-i+1}\right)^i - 1\right)\left(\left(\frac{w-i+k+1}{w-i-k+1}\right)^i - 1\right) \quad (18)$$

$$\leq \left(\left(\frac{w/2+1}{w/2-e+1}\right)^e - 1\right)\left(\left(\frac{3w/2-e+1}{w/2-e+1}\right)^e - 1\right) \quad (19)$$

where the transition from (15) to (16) is by Lemma 6, the transition from (17) to (18) is by Newton's binomial identity, and the transition from (18) to (19) is by using $a \geq 0$, $i \leq e$, and $k \leq w/2$. Therefore, it is enough that we show that

$$\left(\left(\frac{w/2+1}{w/2-e+1}\right)^e - 1\right)\left(\left(\frac{3w/2-e+1}{w/2-e+1}\right)^e - 1\right) < 2. \quad (20)$$

For a fixed value of e

$$\lim_{w\to\infty}\left(\left(\frac{w/2+1}{w/2-e+1}\right)^e - 1\right)\left(\left(\frac{3w/2-e+1}{w/2-e+1}\right)^e - 1\right) = 0$$

and hence, a W_e exists as required. □

We note that Theorem 23 may be easily extended to show that for all $e \geq 2$ and $0 < \epsilon < 1$, there exists $W_{e,\epsilon} > 0$ such that for all $w \geq W_{e,\epsilon}$, all e-perfect codes in $J(2w+a, w)$ are $\lfloor \epsilon w \rfloor$-regular. However, for the following, $\epsilon = 1/2$ is sufficient.

Theorem 24: There are no e-perfect codes in $J(n, w)$, $e \geq 2$, which are also $\lfloor w/2 \rfloor$-regular, when $\Phi_e(n, w) \equiv 0 \pmod 4$.

Proof: Let $\mathcal{C}$ be a $\lfloor w/2 \rfloor$-regular e-perfect code in $J(n, w)$, $n = 2w + a$, for $2^m \leq n \leq 2^{m+1} - 1$. We distinguish between two cases.

Case 1: $2^{m-1} \leq w \leq n/2$. In this case

$$w - 2^{m-1} \leq \frac{w}{2}.$$

Since the code is $\lfloor w/2 \rfloor$-regular, then by Theorem 17

$$\Phi_e(n, w) \left| \binom{n - w + 2^{m-1}}{2^{m-1}}. \right.$$

Theorem 20 implies that

$$\binom{n - w + 2^{m-1}}{2^{m-1}} \not\equiv 0 \pmod 4$$

and so

$$\Phi_e(n, w) \not\equiv 0 \pmod 4.$$

Case 2: $w \leq 2^{m-1} - 1$. Note that by Theorem 13, we also have

$$a < \frac{w - (2e+1)}{e} < \frac{w}{2}.$$

If we want to use Theorem 17, we have to show that

$$n - (2^m - 1) \leq \frac{w}{2}. \quad (21)$$

But now

$$n - \frac{w}{2} = 2w + a - \frac{w}{2} < 2w < 2^m - 1.$$

Hence, (21) holds, and then by Theorem 17

$$\Phi_e(n, w) \left| \binom{2^m - 1}{w - n + 2^m - 1}. \right.$$

Theorem 20 implies that

$$\binom{2^m - 1}{w - n + 2^m - 1} \not\equiv 0 \pmod 4$$

and so

$$\Phi_e(n, w) \not\equiv 0 \pmod 4.$$ □

Theorem 25: There are no e-perfect codes in $J(n, w)$, $e \geq 2$, which are also $\lfloor w/2 \rfloor$-regular, when $\Phi_e(n, w) \equiv 0 \pmod{p^2}$, $p \geq 3$ a prime.

Proof: Let $\mathcal{C}$ be an e-perfect code in $J(n, w)$, for $p^m \leq n \leq p^{m+1} - 1$. Now, if $w \leq p^{m-1} - 1$, then we have $w < n/p$ which is impossible for $p \geq 3$ by Theorem 3. Hence, let $kp^{m-1} \leq w \leq (k+1)p^{m-1} - 1$, for some $1 \leq k \leq p^2 - 1$. In this case

$$w - kp^{m-1} \leq \frac{w}{2}.$$

Since the code is $\lfloor w/2 \rfloor$-regular, then by Theorem 17

$$\Phi_e(n, w) \left| \binom{n - w + kp^{m-1}}{kp^{m-1}}. \right.$$

Theorem 20 implies that

$$\binom{n - w + kp^{m-1}}{kp^{m-1}} \not\equiv 0 \pmod{p^2}$$

and so

$$\Phi_e(n, w) \not\equiv 0 \pmod{p^2}.$$ □

Corollary 11: There are no e-perfect codes in $J(n, w)$, $e \geq 2$, which are also $\lfloor w/2 \rfloor$-regular, when $\Phi_e(n, w) \equiv 0 \pmod{p^2}$, p a prime.

To prove the next theorem we need another interesting theorem on binomial coefficients. This theorem is due to Lucas [22]. Let $a \geq 0$ be some integer. We then denote by $\mathsf{d}_p(a, i)$, the ith digit of a when written in base p. Hence,

$$a = \sum_{i=0}^{\infty} \mathsf{d}_p(a, i) p^i.$$

Theorem 26: Let p be a prime, and $n \geq m \geq 0$ two integers, then

$$\binom{n}{m} \equiv \prod_{i=0}^{\infty}\binom{\mathsf{d}_p(n, i)}{\mathsf{d}_p(m, i)} \pmod p.$$

Theorem 27: Let p be a prime, and $e \equiv -1 \pmod{p^2}$. If an e-perfect code exists in $J(n, w)$, then

$$\Phi_e(n, w) \equiv 0 \pmod{p^2}.$$

Proof: Let $\mathcal{C}$ be an e-perfect code in $J(n, w)$. By Corollary 2, $w + 1 \equiv n - w + 1 \equiv 0 \pmod{e+1}$ and hence $w + 1 \equiv n - w +$

$1 \equiv 0 \pmod{p^2}$. In other words, the two least significant digits in the representation in base p of e, w, and $n-w$, are both $p-1$, i.e.,

$$\begin{aligned}\mathsf{d}_p(w,0) &= \mathsf{d}_p(w,1) = \mathsf{d}_p(n-w,0)\\ &= \mathsf{d}_p(n-w,1)\\ &= \mathsf{d}_p(e,0) = \mathsf{d}_p(e,1) = p-1. \end{aligned} \tag{22}$$

Let $0 \le j < e$ be some integer such that $j \equiv 0 \pmod{p}$. Now

$$\binom{w}{j+1}\binom{n-w}{j+1} = \binom{w}{j}\binom{n-w}{j}\frac{(w-j)(n-w-j)}{(j+1)^2}.$$

However, note that $w-j$, $n-w-j$, and $j+1$ are coprime to p^2. Furthermore, $w-j \equiv n-w-j \equiv -(j+1) \pmod{p^2}$. Hence,

$$\binom{w}{j}\binom{n-w}{j} \equiv \binom{w}{j+1}\binom{n-w}{j+1} \pmod{p^2}.$$

This may be repeated to get

$$\begin{aligned}\binom{w}{j}\binom{n-w}{j} &\equiv \binom{w}{j+1}\binom{n-w}{j+1} \equiv \cdots \equiv\\ &\equiv \binom{w}{j+p-1}\binom{n-w}{j+p-1} \pmod{p^2}. \end{aligned} \tag{23}$$

Now let $0 \le j < e$ be some integer such that $j \equiv 0 \pmod{p^2}$. Note that in all the numbers of the form $j+ip$, when $0 \le i \le p-1$, only the second digit in base p changes while the first digit is always zero. We examine the following sum modulo p using Theorem 26:

$$\begin{aligned}&\sum_{i=0}^{p-1}\binom{w}{j+ip}\binom{n-w}{j+ip}\\ &\quad\equiv \sum_{i=0}^{p-1}\prod_{\ell=0}^{\infty}\left[\binom{\mathsf{d}_p(w,\ell)}{\mathsf{d}_p(j+ip,\ell)}\binom{\mathsf{d}_p(n-w,\ell)}{\mathsf{d}_p(j+ip,\ell)}\right]\\ &\quad\equiv \left(\sum_{i=0}^{p-1}\binom{p-1}{i}^2\right)\\ &\qquad\cdot\left(\prod_{\ell=2}^{\infty}\left[\binom{\mathsf{d}_p(w,\ell)}{\mathsf{d}_p(j+ip,\ell)}\binom{\mathsf{d}_p(n-w,\ell)}{\mathsf{d}_p(j+ip,\ell)}\right]\right)\\ &\quad\equiv \binom{2(p-1)}{p-1}\\ &\qquad\cdot\prod_{\ell=2}^{\infty}\left[\binom{\mathsf{d}_p(w,\ell)}{\mathsf{d}_p(j+ip,\ell)}\binom{\mathsf{d}_p(n-w,\ell)}{\mathsf{d}_p(j+ip,\ell)}\right] \pmod{p}.\end{aligned}$$

However, $\mathsf{d}_p(2(p-1),0) = p-2 < p-1 = \mathsf{d}_p(p-1,0)$, and therefore, by Theorem 20

$$\binom{2(p-1)}{p-1} \equiv 0 \pmod{p}.$$

Hence, the previous sum is congruent to 0 modulo p. Now, for some integer k

$$\sum_{i=0}^{p-1}\binom{w}{j+ip}\binom{n-w}{j+ip} = kp. \tag{24}$$

We continue by examining the following sum modulo p^2:

$$\begin{aligned}&\sum_{i=0}^{p^2-1}\binom{w}{j+i}\binom{n-w}{j+i}\\ &\quad\equiv \sum_{\ell=0}^{p-1}\sum_{i=0}^{p-1}\binom{w}{j+ip+\ell}\binom{n-w}{j+ip+\ell}\\ &\quad\equiv p\sum_{i=0}^{p-1}\binom{w}{j+ip}\binom{n-w}{j+ip} \quad \text{by (23)}\\ &\quad\equiv kp^2 \quad \text{by (24)}\\ &\quad\equiv 0 \pmod{p^2}.\end{aligned}$$

Finally, using the fact that $e \equiv -1 \pmod{p^2}$, the sphere size modulo p^2 equals

$$\begin{aligned}\Phi_e(n,w) &\equiv \sum_{i=0}^{e}\binom{w}{i}\binom{n-w}{i}\\ &\equiv \sum_{\substack{0\le j<e\\ j\equiv 0 \pmod{p^2}}}\sum_{i=0}^{p^2-1}\binom{w}{j+i}\binom{n-w}{j+i}\\ &\equiv 0 \pmod{p^2}.\end{aligned}$$

□

Corollary 12: For any given $e \ge 2$, $e \equiv -1 \pmod{p^2}$, p prime, there are finitely many nontrivial e-perfect codes in the Johnson graph.

V. Applications

A simple observation is that the left-hand side of (20) is a monotonously decreasing function in w. Hence, a simple computer search can find the value of W_e of Theorem 23 and validate that $\sigma_e(w,a,k)$ has no integer roots for $k \le w/2$ and $w \le W_e$. Such a computer search was done for $e = 3, 7, 8$ and, indeed, no such roots were found. Therefore, we conclude the following.

Proposition 1: There are no nontrivial 3-perfect, 7-perfect, and 8-perfect codes in the Johnson graph.

Another computer search was conducted which tested the divisibility conditions of Theorem 17. The results of this search are given in the next two propositions.

Proposition 2: There are no 1-perfect codes in $J(n,w)$ for all $n \le 50000$.

Proposition 3: There are no 2-perfect codes in $J(n,w)$ for all $n \le 40000$.

This is a significant improvement over the previous method using Steiner systems, which left for $e = 1$ all $w \equiv n-w \equiv 1 \pmod{6}$ as candidates, and for $e = 2$ all $w \equiv n-w \equiv 2, 26, 50 \pmod{60}$ as candidates. We believe that further number-theoretic analysis of the regularity method will rule out all perfect codes.

Finally, for given e and a, we examine in which graphs $J(2w+a,w)$ the existence of e-perfect codes was not ruled out. The results of Sections III and IV and careful analysis show the following.

Theorem 28: For $1 \le a \le 35$, there are no e-perfect codes in $J(2w+a,w)$ with the following possible exceptions: 1-perfect codes and 2-perfect codes in $J(2w+12,w)$ and $J(2w+24,w)$, and 4-perfect codes in $J(2w+15,w)$ and $J(2w+30,w)$.

VI. Conclusion

The main purpose of this correspondence was to attack Delsarte's 30 years old conjecture on the nonexistence of nontrivial perfect codes in the Johnson scheme. We showed various results which rule out e-perfect codes in $J(n,w)$ for various values of e, n, and w. A novel technique using k-regular codes was introduced. For practical use, this technique is able to rule out any given set of parameters.

The main problem that should be the focus of further research is to prove that there are no nontrivial perfect codes in the Johnson scheme by using the concept of k-regular codes.

ACKNOWLEDGMENT

The authors would like to thank the two anonymous referees whose comments have amended this correspondence.

REFERENCES

[1] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1978.

[2] J. H. van Lint, "Nonexistence theorems for perfect error-correcting codes," in *Computers in Algebra and Number Theory, vol. IV, SIAM-AMS Proceedings*, 1971.

[3] A. Tietäväinen, "On the nonexistence of perfect codes over finite fields," *SIAM J. Appl. Math.*, vol. 24, pp. 88–96, 1973.

[4] V. A. Zinoviev and V. K. Leontiev, "The nonexistence of perfect codes over Galois fields," *Probl. Control and Inform. Theory*, vol. 2, pp. 123–132, 1973.

[5] M. R. Best, "Perfect codes hardly exist," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 349–351, May 1983.

[6] Q. A. Nguyen, L. Györfi, and J. L. Massey, "Constructions of binary constant-weight cyclic codes and cyclically permutable codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 940–949, May 1992.

[7] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, "A new table of constant-weight codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1334–1380, Nov. 1990.

[8] F. R. K. Chung, J. A. Salehi, and V. K. Wei, "Optical orthogonal codes: Design, analysis, and applications," *IEEE Trans. Inform. Theory*, vol. 35, pp. 595–604, May 1989.

[9] T. Etzion, "Constructions of error-correcting DC-free block codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 899–905, July 1990.

[10] H. C. A. van Tilborg and M. Blaum, "On error-correcting balanced codes," *IEEE Trans. Inform. Theory*, vol. 35, pp. 1091–1095, Sept. 1989.

[11] P. Delsarte, "An algebraic approach to association schemes of coding theory," *Philips J. Res.*, vol. 10, pp. 1–97, 1973.

[12] E. Biggs, "Perfect codes in graphs," *J. Combin. Theory Ser. B*, vol. 15, pp. 289–296, 1973.

[13] E. Bannai, "Codes in bi-partite distance-regular graphs," *J. London Math. Soc.*, vol. 2, pp. 197–202, 1977.

[14] P. Hammond, "On the nonexistence of perfect codes and nearly perfect codes," *Discr. Math.*, vol. 39, pp. 105–109, 1982.

[15] C. Roos, "A note on the existence of perfect constant weight codes," *Discr. Math.*, vol. 47, pp. 121–123, 1983.

[16] T. Etzion, "On the nonexistence of perfect codes in the Johnson scheme," *SIAM J. Discr. Math.*, vol. 9, no. 2, pp. 201–209, May 1996.

[17] ——, "On perfect codes in the Johnson scheme," *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, vol. 56, pp. 125–130, 2001.

[18] W. J. Martin, "Completely regular subsets," Ph.D. dissertation, Univ. Waterloo, Waterloo, ON, Canada, 1992.

[19] O. Shimabukuro, "On the nonexistence of perfect codes in $J(2w+p^2, w)$," *Ars Combinatoria*, to be published.

[20] R. Ahlswede, H. K. Aydinian, and L. H. Khachatrian, "On perfect codes and related concepts," *Des., Codes Cryptogr.*, vol. 22, no. 3, pp. 221–237, Jan. 2001.

[21] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*. Reading, MA: Addison-Wesley, 1994.

[22] N. J. Fine, "Binomial coefficients modulo a prime," *Amer. Math. Monthly*, vol. 54, pp. 589–592, 1947.

Cocyclic Simplex Codes of Type α Over $\boldsymbol{Z}_4$ and $\boldsymbol{Z}_{2^s}$

Nimalsiri Pinnawala and Asha Rao

***Abstract*—Over the past decade, cocyles have been used to construct Hadamard and generalized Hadamard matrices. This, in turn, has led to the construction of codes—self-dual and others. Here we explore these ideas further to construct cocylic complex and Butson–Hadamard matrices, and subsequently we use the matrices to construct simplex codes of type α over $\boldsymbol{Z}_4$ and $\boldsymbol{Z}_{2^s}$, respectively.**

***Index Terms*—Butson, cocycle, complex Hadamard, exponent, quaternary, self-orthogonal, simplex codes, trace.**

I. INTRODUCTION

Various authors [1], [2], [11], [12] have studied the construction of cocyclic Hadamard and cocyclic generalized Hadamard matrices and the use of these matrices in the construction of cocyclic codes. Here we extend these constructions to obtain cocyclic Butson and cocyclic complex Hadamard matrices. Simplex codes of type α were studied by Gupta [9], but no methods of constructions were given. We use the cocyclic complex and cocyclic Butson–Hadamard matrices to construct simplex codes of type α over $\boldsymbol{Z}_4$ and $\boldsymbol{Z}_{2^s}$, respectively. We assume that the reader is familiar with the basic facts of the theory of Hadamard matrices (see, for example, [15]) and of binary linear codes (see [13]).

If G is a finite group (written multiplicatively with identity 1) and C is an Abelian group, a *cocycle* (over G) is a set mapping $\psi: G\times G \to C$ which satisfies

$$\psi(a,b)\psi(ab,c) = \psi(a,bc)\psi(b,c), \qquad \forall a,b,c \in G.$$

A cocycle is *normalized* if $\psi(1,1) = 1$. A cocycle may be represented as a cocyclic matrix $M_\psi = [\psi(a,b)]_{a,b\in G}$ once an indexing of the elements of G has been chosen.

Let C_p be the multiplicative group of all complex pth roots of unity, $C_p = \{1, x, x^2, \ldots, x^{p-1}\}$, where $x = \exp(2\pi i/p)$ and $p \geq 2$ is an integer. A square matrix $H = [h_{ij}]$ of order n with elements from C_p is called a Butson–Hadamard matrix $(BH(n,p))$ (see [5]) if and only if $HH^* = nI$, H^* being the conjugate transpose of H and I the identity matrix of order n. When $p = 2$ and $n = 1, 2$ or a multiple of 4, $BH(n,p)$ is a Hadamard matrix.

A complex Hadamard matrix H of order n is a matrix with entries from $\{1, i, -1, -i\}$ that satisfies $HH^* = nI$, where $i = \sqrt{-1}$ and H^* is the conjugate transpose of H. It is conjectured that a complex Hadamard matrix exists for every even order. In [15], it is shown that every complex Hadamard matrix has order 1 or divisible by 2. A complex Hadamard matrix is a special case of a Butson–Hadamard matrix $BH(n,p)$ for $p = 4$.

Let $H = [h_{i,j}]$ be a square matrix over C_p, where p is a fixed integer $p > 2$. The matrix $E = [e_{i,j}]$, $e_{i,j} \in \boldsymbol{Z}_p$, which is obtained from $H = [x^{e_{i,j}}] = [h_{i,j}]$, where $x = \exp(2\pi i/p)$, is called the *exponent matrix* associated with H. The elements of the exponent matrix E lie in the Galois ring GR $(p, 1)$ (Galois field GF (p), for p prime), and its row vectors can be viewed as the codewords of a code over the integers modulo p.

Manuscript received December 10, 2003; revised May 5, 2004.

The authors are with the Department of Mathematics and Statistics, Royal Melbourne Institute of Technology, GPO Box 2476V, Melbourne, VIC 3001, Australia.

Communicated by C. Carlet, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2004.833354