ON THE NONEXISTENCE OF PERFECT CODES IN THE JOHNSON SCHEME*

TUVI ETZIONI

Abstract. Although it was conjectured by Delsarte in 1973 that no nontrivial perfect codes exist in the Johnson scheme, only very partial results are known. In this paper we considerably reduce the range in which perfect codes in the Johnson scheme can exist; e.g., we show that there are no nontrivial perfect codes in the Johnson graph $J(2w + p, w)$, $p$ prime. We give theorems about the structure of perfect codes if they exist. This involved structure gives more evidence in support of the belief that no nontrivial perfect codes exist in the Johnson scheme.

Key words. perfect code, Steiner system, Hamming scheme, Johnson graph, Johnson scheme

AMS subject classifications. 05B15, 05B30, 51E10, 94B25

1. Introduction. Perfect codes always draw the attention of coding theorists and mathematicians. They are defined on large varieties of metrics, e.g., Hamming, Johnson, and Lee [7]. Although a lot of results are known regarding the Hamming metric [4], [7], and the Lee metric [5], [7] (and we don’t give the enormous number of references in order to save space), only a few results are known on perfect codes in the Johnson metric.

In the Johnson scheme, we are given two integers, $n$ and $w$, such that $0 \leq w \leq n$. Given a binary code $C$, all its codewords have length $n$ and constant weight $w$. Two codewords $u$ and $v$ are in distance $(J$-distance) $d$ apart if there are exactly $d$ positions in which $u$ has $1$ value and $v$ has $0$ values. Obviously, there are exactly $d$ other positions in which $u$ has $0$ values and $v$ has $1$ value. With the Johnson scheme we associate the Johnson graph $J(n, w)$. The vertex set $V^n_w$ 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 $C$ of such $w$-subsets is called e-perfect code in $J(n, w)$ (or in the Johnson scheme) if the $e$-spheres of all the codewords of $C$ form a partition of $V^n_w$. In other words, $C$ is an e-perfect code if for each element $v \in V^n_w$ there exists a unique element $c \in C$, such that the J-distance between $v$ and $c$ is less than or equal to $e$. There are some trivial perfect codes in $J(n, w)$.

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

Delsarte [3, p. 55] conjectured that $J(n, w)$ doesn’t contain nontrivial perfect codes. Bannai [1] proved the nonexistence of e-perfect codes in $J(2w - 1, w)$ and $J(2w + 1, w)$ for $e \geq 2$. Hammond [6] extended the result and showed that $J(n, w)$ cannot contain a nontrivial perfect code for $n \in \{2w - 2, 2w - 1, 2w + 1, 2w + 2\}$. Generalizations of Lloyd’s theorem [1], [3], didn’t lead to significant results. A significant improvement was made by Roos [8] who showed the following result.

THEOREM 1.1. If an e-perfect code in $J(n, w)$, $n \geq 2w$, exists, then $n \leq (w - 1)(2e + 1)/e$.

* Received by the editors October 10, 1994; accepted for publication (in revised form) April 5, 1995. This research was supported in part by Science and Engineering Research Council (United Kingdom) grant GR/K01605.
† Computer Science Department, Royal Holloway College, University of London, Egham, Surrey TW20 0EX, UK. The author is on leave of absence from the Computer Science Department, Technion–Israel Institute of Technology, Haifa 32000, Israel.
In this paper we make a considerable improvement on the range in which perfect codes cannot exist. We show that there are strong connections between perfect codes and Steiner systems. If nontrivial perfect code exists then many Steiner systems are embedded in it. They are embedded in such an involved way that it seems impossible that such a structure can exist. The necessary conditions on the existence of these Steiner systems reduce the range in which these perfect codes can exist.

This paper is organized as follows. In §2 we introduce the necessary notation and definitions on codes and Steiner systems that are needed for our discussion. We also give some simple results that are essential for the discussion. In §3 we give two theorems that connect the existence of perfect codes with the existence of Steiner systems. The proofs of these theorems reveal the involved structure of the perfect codes. In §4 we prove that, except for the trivial perfect codes, there cannot exist perfect codes which are also Steiner systems. In §5 we give a concept similar to the weight distribution on e-perfect codes in the Johnson scheme. Using this concept we will show that there are no e-perfect codes in $J(2w + e + 1, w)$. In §6 we examine the theorems of §§3, 4, and 5 to show that the range in which e-perfect codes exist is considerably reduced. We also explore the involved structure obtained in §3.

2. Notation, definitions, and preliminaries. Perfect codes in the Johnson scheme have a strong connection to constant weight codes and Steiner systems. For this purpose we need to use the Hamming metric. Two binary words $u$ and $v$ of the same length $n$ have Hamming distance (H-distance) $d$ if they differ in exactly $d$ positions. Note that two words $u, v \in V^n_w$ have J-distance $d$ if and only if their H-distance is $2d$. A code $C$ has minimum H-distance $d$ if for any two codewords $u, v \in C$, the H-distance between $u$ and $v$ is at least $d$.

**Lemma 2.1.** If $C$ is an e-perfect code in the Johnson scheme then its minimum H-distance is $4e + 2$.

**Proof.** Since $C$ is an e-perfect code, it follows that the e-spheres of two words with J-distance less than $2e + 1$ have nonempty intersection. Hence, the minimum J-distance of the code is $2e + 1$ and its minimum H-distance is $4e + 2$. □

An $(n, d, w)$ code is a code of length $n$, constant weight $w$ to all the codewords, and minimum H-distance $d$. $A(n, d, w)$ denote the maximum size of an $(n, d, w)$ code. An extensive survey on the lower bounds on $A(n, d, w)$ can be found in [2].

**Lemma 2.2.** If $C$ is an e-perfect code in $J(n, w)$ then $A(n, 4e + 2, w) = |C|$.

**Proof.** Assume $C$ is an e-perfect code in $J(n, w)$. By Lemma 2.1 $C$ has minimum H-distance $4e + 2$, and hence it is an $(n, 4e + 2, w)$ code. Given an $(n, 4e + 2, w)$ code, in the Johnson scheme, its minimum J-distance is $2e + 1$ and hence the e-spheres around its codewords are disjoint. The lemma follows from the facts that all e-spheres in $J(n, w)$ have the same size and in an e-perfect code they form a partition of $V^n_w$. □

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 theorem is well known, e.g., [7, p. 60].

**Theorem 2.3.** A necessary condition that a Steiner system $S(t, k, n)$ exists is that the numbers $\left(\binom{n-i}{t-i}/\binom{k-i}{t-i}\right)$ be integers for $0 \leq i \leq t$.

Henceforth, let $N = \{1, 2, \ldots, n\}$ be the $n$-set. From a Steiner system $S(t, k, n)$ we construct constant weight code on $n$ coordinates as follows. From each block $B$ we construct a codeword with 1's in the positions of $B$ and 0's in the positions of $N \setminus B$. This construction leads to the following well-known theorem [2].
THEOREM 2.4. \( A(n, 2(k-t+1), k) = \frac{n(n-1) \ldots (n-(t+1))}{k(k-1) \ldots (k-(t+1))} \) if and only if a Steiner system \( S(t, k, n) \) exists.

From Theorem 2.4 and Lemma 2.1 we immediately infer the following result.

LEMMA 2.5. If \( C \) is an e-perfect code in \( J(n, w) \) and is also a Steiner system then it is a Steiner system \( S(w-2e, w, n) \).

COROLLARY 2.6. If \( C \) is an e-perfect code in \( J(n, w) \) which is not a Steiner system \( S(w-2e, w, n) \) then there exists at least one set of \( w-2e \) coordinates which are not contained in any codeword.

LEMMA 2.7. The complement of an e-perfect code in \( J(n, w) \) is an e-perfect code in \( J(n, n-w) \).

Proof. This lemma is a simple observation from the fact that \( J(n, w) \) and \( J(n, n-w) \) are isomorphic under the mapping which maps each vertex to its complement. \( \square \)

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 \( N \) into two subsets \( A \) and \( B \) such that \( |A| = k \) and \( |B| = n-k \), let configuration \((i, j)\) consist of all vectors with weight \( i \) in the positions of \( A \) and weight \( j \) in the positions of \( B \). For an e-perfect code \( C \) in \( J(n, w) \) we say that \( u \in C \) J-cover \( v \in V_w^n \) if the J-distance between \( u \) and \( v \) is less than or equal to \( e \). For a given two subsets \( u \) and \( v \) we say that \( u \) J-cover \( v \) if \( v \) is a subset of \( u \) (this is our usual understanding of the word cover).

In the sequel we will use a mixed language of set and vector notations. It should be understood from the context which one we are using and the translation between the two different notations.

3. Perfect codes and Steiner systems. In this section we will prove that if there exists an e-perfect code in the Johnson scheme, then many Steiner systems are embedded in it. This fact will force the necessary conditions for the existence of these Steiner systems also to become necessary conditions for the existence of the e-perfect codes. The involved way in which these Steiner systems are embedded in the perfect codes will make it reasonable to believe that except for the trivial perfect codes no other e-perfect codes exist in the Johnson scheme.

THEOREM 3.1. If an e-perfect code in \( J(n, w) \) exists, then a Steiner system \( S(e+1, 2e+1, w) \) exists.

Proof. Assume \( C \) is an e-perfect code in \( J(n, w) \). We partition \( N \) into two subsets \( A \) and \( B \), such that \( |A| = w \), \( |B| = n-w \), and the vector of the \((w, 0)\) configuration is a codeword. This codeword J-covers exactly all the vectors of all configurations \((w-x, x)\), where \( 0 \leq x \leq e \). Since \( C \) is e-perfect code and all vectors of all configurations \((w-x, x)\), \( 0 \leq x \leq e \), are covered, it follows that \( C \) does not contain any codeword of any configurations \((w-x, x)\), where \( 1 \leq x \leq 2e \). Therefore, all words of configuration \((w-e-1, e+1)\) must be J-covered by codewords from configuration \((w-2e-1, 2e+1)\). Consider now all \( \binom{w}{e+1} \) vectors in configuration \((w-e-1, e+1)\) with \( e+1 \) 1's in \( e+1 \) fixed positions of \( B \). These vectors are J-covered by codewords from configuration \((w-2e-1, 2e+1)\) with \( 2e+1 \) 1's in positions of \( B \) which C-covers the \( e+1 \) fixed positions. Let \( C_1 \) be this set of codewords. Each subset of \( e+1 \) 0's in \( A \) with these \( e+1 \) fixed positions in \( B \) must be C-covered and no subset can be C-covered twice (since the code is perfect). Hence, the complement of the A part of \( C_1 \) forms a Steiner system \( S(e+1, 2e+1, n-w) \).

\( \square \)

By using Lemma 2.7 we also have the following corollary.

COROLLARY 3.2. If an e-perfect code in \( J(n, w) \) exists, then a Steiner system \( S(e+1, 2e+1, n-w) \) exists.
Theorem 3.3. If an e-perfect code in $J(n, w)$, which is not a Steiner system $S'(w - 2e, w, n)$, exists then for some $k$, $0 \leq k \leq e - 1$, a Steiner system $S(2, 2e - k + 1, n - w + 2e - 2k)$ exists.

Proof. The proof will be given in some kind of inductive approach. Assume $C$ is an e-perfect code in $J(n, w)$ which is not a Steiner system $S'(w - 2e, w, n)$. We partition $N$ into two subsets, $A_0$ and $B_0$, such that $|A_0| = w - 2e, |B_0| = n - w + 2e$, and there are no codewords in $C$ from configuration $(w - 2e, 2e)$, but there is at least one codeword from configuration $(w - 2e - 1, 2e + 1)$. This can be done as a simple consequence from Corollary 2.6. For a given $k, 0 \leq k \leq e - 2$, assume $N$ is partitioned into two subsets $A_k$ and $B_k$, such that $|A_k| = w - 2e + 2k, |B_k| = n - w + 2e - 2k$, there are no codewords in $C$ from any configuration $(w - 2e + i, 2e - i), k \leq i \leq 2k$, but there is at least one codeword from configuration $(w - 2e + k - 1, 2e - k + 1)$. Let $C_k$ be the set of codewords from configuration $(w - 2e + k - 1, 2e - k + 1)$. In the $B_k$ part of $C_k$ we search for two coordinates in which each codeword has at least one 0. If none exist then the $B_k$ part forms a Steiner system $S(2, 2e - k + 1, n - w + 2e - 2k)$ (note, that if two codewords of $C_k$ have two 1’s in the same two coordinates of the $B_k$ part their H-distance will be $4e$, contradicting Lemma 2.1). If these two coordinates exist, we join them to $A_k$ to obtain $A_{k+1}$ and $B_{k+1} = N \setminus A_{k+1}$. Now, $|A_{k+1}| = w - 2e + 2(k + 1), |B_{k+1}| = n - w + 2e - 2(k + 1)$, and there are no codewords in $C$ from any configuration $(w - 2e + i, 2e - i), k + 1 \leq i \leq 2(k + 1)$, but there is at least one codeword from configuration $(w - 2e + k, 2e - k)$. If $k = e - 2$ and we obtain $|A_{e-1}| = w - 2, |B_{e-1}| = n - w + 2$, there are no codewords in $C$ from any configuration $(w - 2e + i, 2e - i), e - 1 \leq i \leq 2e - 2$, but there is at least one codeword in $C$ from configuration $(w - e - 2, e + 2)$. This means that vectors of configuration $(w - 2, 2)$ can be J-covered only by codewords of configuration $(w - e - 2, e + 2)$. Since each vector of configuration $(w - 2, 2)$ is J-covered exactly once, it follows that the $B_{e-1}$-part of the codewords from configuration $(w - e - 2, e + 2)$ forms a Steiner system $S(2, e + 2, n - w + 2)$. □

Corollary 3.4. If an e-perfect code in $J(n, w)$, which is not a Steiner system $S(n - w - 2e, n - w, n)$, exists then for some $k$, $0 \leq k \leq e - 1$, a Steiner system $S(2, 2e - k + 1, w - 2e - 2k)$ exists.

4. Only trivial Steiner systems are perfect codes. As said before, for $n = 2w, w$ odd, any pair of disjoint $w$-subsets is e-perfect with $e = \frac{3}{2}(w - 1)$. These two $w$-subsets form a Steiner system $S(1, w, n)$. For any $n$ and $1 \leq w \leq n$, $V_w^n$ is 0-perfect, and it forms a Steiner system $S(w, w, n)$. A natural question is whether there exist more perfect codes which are also Steiner systems. The answer to this question is our next theorem. But, first we need the following simple lemma.

Lemma 4.1. If a Steiner system $S(w - k, w, n), k \geq 1$, exists then $n \geq 2w$.

Proof. Assume $n < 2w$ and a Steiner system $S(w - k, w, n), k \geq 1$, exists. The number of blocks in this system is

$$\binom{n}{w-k} = \frac{n! \cdot k!}{(n-w+k)! \cdot w!}.$$ 

The number of blocks in a packing of $(n-w)$-subsets of $N$ in which each $(n-w-k)$-subset of $N$ is contained in at most one block is less than or equal to

$$\frac{n! \cdot k!}{(n-k)! \cdot (n-w)!}.$$
If \( n < 2w \) and \( k \geq 1 \) then obviously
\[
\frac{\binom{n}{w-k}}{\binom{w}{w-k}} > \frac{\binom{n-w}{w-k}}{\binom{n-w}{w-k}}.
\]
But since the complement of the code derived from the Steiner system \( S(w-k, w, n) \) is a packing of \((n-w)\)-subsets of \( N \) in which each \((n-w-k)\)-subset of \( N \) is contained at most in one block, we have a contradiction. Hence, if a Steiner system \( S(w-k, w, n) \), \( k \geq 1 \), exists then \( n \geq 2w \).

**Theorem 4.2.** 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.

**Proof.** Assume \( C \) is an \( e \)-perfect code in \( J(n, w) \) which is also a Steiner system. Since \( C \) is \( e \)-perfect it follows by Lemma 2.1 that \( C \) has minimum \( H \)-distance \( 4e + 2 \), and by Lemma 2.5 it is a Steiner system \( S(w-2e, w, n) \). Now, we partition \( N \) into two subsets \( A \) and \( B \) such that \( |A| = w - 2e + 1, |B| = n - w + 2e - 1 \), and there is no codeword in \( C \) from configuration \((w-2e+1, 2e-1)\). Since \( C \) is a Steiner system \( S(w-2e, w, n) \) and no word in \( C \) is from configuration \((w-2e+1, 2e-1)\), it follows that there are \( w-2e+1 \) codewords in \( C \) from configuration \((w-2e, 2e)\). Since the minimum \( H \)-distance of \( C \) is \( 4e + 2 \) it follows that the \( 2e \) elements in \( B \), of any two codewords from configuration \((w-2e, 2e)\), must be disjoint. Hence, we have \( n \geq (w-2e+1) + (w-2e+1)2e = (w-2e+1)(2e+1) \). By Lemma 4.1, \( n \geq 2w \), and hence by Theorem 1.1 we have \((w-1)(2e+1)/e \geq n \), and therefore
\[
(w-1)(2e+1)/e \geq (w-2e+1)(2e+1).
\]

We now distinguish between two cases.

**Case 1.** For \( e > 1 \) this implies \( 2e + 1 \geq w \) Therefore, the intersection between any two codewords is empty since the minimum \( H \)-distance is \( 4e + 2 \). Thus, the code contains two codewords, \( n = 2w \), and the Steiner system is \( S(1, w, n) \).

**Case 2.** For \( e = 1 \) this implies \( n = 3w - 3 \). By Theorem 3.1 a Steiner system \( S(2, 3, w) \) exists and hence by Theorem 2.3, \( w \equiv 1 \) or \( 3 \pmod{6} \). Therefore, we have \( n \equiv 0 \pmod{6} \). By Corollary 3.2, Steiner system \( S(2, 3, n-w) \) exists also and hence by Theorem 2.3, \( n-w \equiv 1 \) or \( 3 \pmod{6} \). By Theorem 3.3 a Steiner system \( S(2, 3, n-w+2) \) exists also and hence by Theorem 2.3, \( n-w+2 \equiv 1 \) or \( 3 \pmod{6} \) which implies that \( n-w \equiv 1 \pmod{6} \). Since \( n \equiv 0 \pmod{6} \), it follows that \( w \equiv 5 \pmod{6} \), a contradiction.

Thus, no nontrivial perfect code is a Steiner system.

**5. No \( e \)-perfect codes in \( J(2w+e+1, w) \).** By Theorem 3.1 and Corollary 3.2, if an \( e \)-perfect code exists in \( J(n, w) \) then Steiner systems \( S(e+1, 2e+1, w) \) and \( S(e+1, 2e+1, n-w) \) exist. By the divisibility conditions of Theorem 2.3 this implies that \( e+1 \) divides \( w-e \) and \( n-w-e \), i.e., \( n-w \equiv w \equiv e \pmod{e+1} \). This implies that \( e \)-perfect codes might exist in \( J(2w+e+1, w) \). In this section we prove that no nontrivial \( e \)-perfect codes exist in \( J(2w+e+1, w) \). This result and the results of the previous sections enable us to show many Johnson graphs in which no nontrivial perfect codes exist. The proof will proceed in a few steps which also show some properties of \( e \)-perfect codes if they exist. Assume \( C \) is an \( e \)-perfect code in \( J(n, w) \) and \( N \) is partitioned into two parts \( A \) and \( B \) such that \( |A| = w \) and \( |B| = n-w \). Let \( D(i, j) : 0 \leq i, j, i+j=w \) denote the configuration distribution of the code; i.e., \( D(i, j) \) denote the number of codewords from configuration \((i,j)\).
THEOREM 5.1. There are exactly $e + 1$ different configuration distributions for an $e$-perfect code. If $W_k$, $0 \leq k \leq e$, is the set of the $k$th configuration distribution then $W_k$ contains $D_{(w-k,k)}$ and $D_{(w-2e-1+k, 2e+1-k)}$ as the only nonzero elements among $D_{(w-i,i)}$, $0 \leq i \leq 2e + 1 - k$.

Proof. Let $k$ be the smallest integer such that $C$ has a codeword from configuration $(w-k, k)$. Since we must $J$-cover the vector from configuration $(w, 0)$, it follows that $0 \leq k \leq e$. Since by Lemma 2.1 the minimum H-distance of $C$ is $4e + 2$, it follows that there is exactly one codeword from configuration $(w-k, k)$ and no codewords from any configuration $(w-j, j)$, $k + 1 \leq j \leq 2e - k$. The codeword from configuration $(w-k, k)$ J-covers all vectors from configurations $(w-i, i)$ for all $i$, $0 \leq i \leq e - k$. Vectors from configurations $(w-e+k-1, e+k+1)$ are J-covered by the codeword from the $(w-k, k)$ configuration if $k > 0$, and the rest, which are the most, can be J-covered only by codewords from configuration $(w-2e-1+k, 2e+1-k)$. Note, that we can always partition $N$ into $A$ and $B$ such that the first codeword will have $w-k$ 1's in $A$ and $k$ 1's in $B$, and hence $C$ contains a codeword from configuration $(w-k, k)$. To complete the proof we have to show that once we are given $k$, $0 \leq k \leq e$, such that a codeword from configuration $(w-k, k)$ is in the code (i.e., $D_{(w-k, k)} = 1$, $D_{(w-i, i)} = 0$, $0 \leq i \leq 2e - k$, $i \neq k$), then the configuration distribution is determined. The proof is by induction; assume we have determined all the values $D_{(w-i, i)}$, $0 \leq i \leq r$, for some $r$, $r \geq 2e - k$, and all vectors from configurations $(w-j, j)$, $0 \leq j \leq r - e$, are J-covered by codewords from configurations $(w-i, i)$, $0 \leq i \leq r$. To evaluate $D_{(w-r+1, r+1)}$ notice that by considering how vectors of configuration $(w-r+e-1, r-e+1)$ are J-covered we have

$$\binom{w}{r-e+1} \binom{n-w}{r-e+1} = \sum_{i=r-2e+1}^{r+1} C_{(w-i, i)} D_{(w-i, i)}$$

where $C_{(x_1, y_1)}$ is the number of vectors from configuration $(x_1, y_1)$ which are J-covered by a codeword from configuration $(x_1, y_1)$. Hence we have

$$D_{(w-r+1, r+1)} = \frac{\binom{w}{r-e+1} \binom{n-w}{r-e+1} - \sum_{i=r-2e+1}^{r} C_{(w-i, i)} D_{(w-i, i)}}{C_{(w-r+1, r-e+1)} D_{(w-r, r+1)}}$$

and hence $D_{(w-r+1, r+1)}$ is determined, and all vectors from configurations $(w-j, j)$, $0 \leq j \leq r - e + 1$, are J-covered by codewords from configurations $(w-i, i)$, $0 \leq i \leq r + 1$.

Thus, there are exactly $e + 1$ different configuration distributions for $e$-perfect codes.

□

LEMMA 5.2. In an $e$-perfect code in $J(2w+e+1, w)$ the intersection between any two codewords is at least $e$.

Proof. Assume $C$ is an $e$-perfect code in $J(2w+e+1, w)$, $N$ is partitioned into two parts $A$ and $B$ such that $|A| = w$, $|B| = w + e + 1$, and $C$ contains the vector $v$, from configuration $(0, w)$, which ends with $e+1$ 0's as a codeword. The only vectors from configuration $(0, w)$ which are not J-covered by this codeword are the $\binom{w}{e+1}$ vectors which end with $e+1$ 1's. Since by Lemma 2.1 any codeword which J-covers some of these vectors should have H-distance at least $4e + 2$ from $v$, it follows that these vectors are J-covered by codewords from configuration $(e, w-e)$, which end with $e+1$ 1's. Moreover, note that since $D_{(0, w)} = 1$ all the configuration distribution of $C$ is determined (as in the proof of Theorem 5.1). Now, by Theorem 5.1, for this
configuration distribution we have $D_{(w-k,k)} = 1$ for exactly one $k$, $0 \leq k \leq e$, and for $i \neq k$, $0 \leq i \leq 2e-k$, $D_{(w-i,i)} = 0$. If $k < e$ we can exchange one column from $A$, with $1$ in the codeword from configuration $(w-k,k)$, with a column from $B$, with $0's$ in the codewords from configurations $(w-k,k)$ and $(0,w)$. The obtained $e$-perfect code $C'$ has $D_{(0,w)} = 1$ and $D_{(w-k-1,k+1)} = 1$, $k+1 \leq e$, a contradiction to the fact that $D_{(0,w)} = 1$ determines all the configuration distribution. Thus, $D_{(w-e,e)} = 1$ and $D_{(w-i,i)} = 0$ for $0 \leq i \leq e-1$. Now, assume that there exists a codeword from configuration $(w-k-r, k+r)$, $k < e$, $r > 0$, which intersects the codeword from configuration $(0,w)$ in exactly $k$ positions. Again, we can exchange $r$ columns from $A$, with $0's$ in the codeword from configuration $(w-k-r, k+r)$, with $r$ columns from $B$ with $1's$ in this codeword and $0's$ in the codeword from configuration $(0,w)$. The obtained $e$-perfect code $C'$ have $D_{(0,w)} = 1$ and $D_{(w-k,k)} = 1$, for $k < e$, a contradiction. Now, note that any codeword can be chosen as the codeword from configuration $(0,w)$ and hence the intersection of any two codewords is at least $e$.

**Theorem 5.3.** There is no $e$-perfect code in $J(2w+e+1, w)$.

**Proof.** Assume $C$ is an $e$-perfect code in $J(2w+e+1, w)$ and $N$ is partitioned into two parts $A$ and $B$ such that $|A| = w$, $|B| = w+e+1$, and $C$ contains the vector from configuration $(w,0)$ as a codeword. By Lemma 5.2 the intersection between any two codewords is at least $e$ and hence $C$ cannot contain a codeword from any configuration $(i,w-i), 0 \leq i \leq e-1$. Therefore, the $\binom{w+e+1}{e+1}$ vectors from configuration $(0,w)$ are $J$-covered only by codewords from configuration $(e,w-e)$. Moreover, every set of $e+1$ positions in the $B$ part must be $C$-covered by the $0's$ of exactly one codeword from configuration $(e,w-e)$. Let $C_1$ be the set of codewords from configuration $(e,w-e)$. Thus, the complement of the $B$ part of $C_1$ forms a Steiner system $S(e+1,2e+1,w+e+1)$.

Each set of $e$ columns of the $B$ part of $C_1$ has exactly $\binom{w+1}{e+1}$ rows with $e$ $0's$, since the complement of the $B$ part of $C_1$ is an $S(e+1,2e+1,w+e+1)$. By exchanging any $e$ columns from $B$ with $e$ columns of $A$ that contain $e$ $1's$ from the codewords of $C_1$ we obtain an $e$-perfect code $C'$. Since $C$ has a codeword from configuration $(w,0)$ it follows that $C'$ has a codeword from configuration $(w-e,e)$. Also, note that $C'$ contains a codeword from configuration $(0,w)$. Clearly, not all $e$ columns of $A$ have $e$ $1's$ in the codewords of $C_1$. If we exchange any $e$ columns of $B$ with $e$ columns of $A$ that do not contain $e$ $1's$ in the codewords of $C_1$ we obtain a code $C''$ with a codeword from configuration $(w-e,e)$ but no codeword from configuration $(0,w)$. This is in contradiction to Theorem 5.1 that all codes with a codeword from configuration $(w-e,e)$ have the same configuration distribution.

Thus, there is no $e$-perfect code in $J(2w+e+1, w)$.

Another interesting consequence from Theorem 5.1 is on the structure of $e$-perfect codes in $J(2w,w)$. We show now that these codes, if they exist, are self-complement; i.e., the complement of the code is equal to the code.

**Theorem 5.4.** An $e$-perfect code in $J(2w,w)$ is self-complement.

**Proof.** Let $C$ be an $e$-perfect code in $J(2w,w)$, and assume $N$ is partitioned into two parts $A$ and $B$ such that $|A| = |B| = w$ and the vector from configuration $(w,0)$ is a codeword. By Theorem 5.1 for exactly one $k$, $0 \leq k \leq e$, we have $D_{(k,w-k)} = 1$ and for $i \neq k$, $0 \leq i \leq 2e-k$, $D_{(i,w-i)} = 0$. If $k > 0$ then we can exchange one column from $B$ with $0's$ in the codeword from configuration $(k,w-k)$ with a column from $B$ with $0's$ in the codeword from configuration $(k,w-k)$ to obtain a new $e$-perfect code $C'$. In $C'$ we have $D_{(w-1,1)} = 1$ and $D_{(k,w-k)} = 1$ in contradiction to the unique configuration distribution when $D_{(k,w-k)} = 1$, $0 \leq k \leq e$, obtained in Theorem 5.1.
Thus, $k = 0$ and $C$ is self-complement. \hfill \Box

6. Applications. The theorems obtained in §§3, 4, and 5 make it possible to reduce the range in which perfect codes in the Johnson scheme can exist. If an $e$-perfect code in $J(n, w)$ exists then by Theorem 3.1 and Corollary 3.2 Steiner systems

$S(e + 1, 2e + 1, w)$ and $S(e + 1, 2e + 1, n - w)$ exist. By the divisibility conditions of Theorem 2.3 we have that $e + 1$ should divide $w - e$ and $n - w - e$ and hence we have $w = e \pmod{e + 1}$. This condition itself limits the range in which e-perfect codes can exist. Combining this condition with the nonexistence of e-perfect codes in $J(2w + e + 1, w)$ obtained in Theorem 5.3 we have the following theorem.

**Theorem 6.1.** There are no perfect codes in $J(2w + p, w)$, $p$ prime.

In fact, we can obtain many more results similar to Theorem 6.1; e.g., there are no perfect codes in $J(2w + 2p, w)$, $p$ prime, $p \neq 3$ or there are no perfect codes in $J(2w + 3p, w)$, $p$ prime, $p \neq 2$, $p \neq 3$, and $p \neq 5$, and other similar theorems. The proofs involve carefully examining the divisibility conditions of Theorem 2.3 for

$S(e + 1, 2e + 1, w)$ and $S(e + 1, 2e + 1, n - w)$, and using Theorem 5.3. Theorem 6.1 immediately implies the results of Bannai [1] and Hammond [6], that there are no nontrivial perfect codes in $J(2w - 2, w)$, $J(2w - 1, w)$, $J(2w + 1, w)$, and $J(2w + 2, w)$. Together with the other divisibility conditions we have that the range is considerably reduced. By Theorem 4.2 we know that a nontrivial $e$-perfect code cannot be a Steiner system. Hence, we can apply Corollary 3.4 and obtain that if there exists an $e$-perfect code in $J(n, w)$ then there exists a Steiner system $S(2, 2e + 1 - k, w + 2e - k)$ for some $k$, $0 \leq k \leq e - 1$. This implies that $C$ is an $e$-perfect code in $J(n, w)$ if $w$ is an admissible value for the necessary conditions for the existence of $S(e + 1, 2e + 1, w)$, and also an admissible value for the necessary conditions of one Steiner system $S(2, 2e + 1 - k, w + 2e - k)$. The same results are applied also on $n - w$ instead of $w$. Checking all these conditions we obtain that for $e = 1$, we must have $n - w \equiv w \equiv 1 \pmod{6}$, for $e = 2$, we have $n - w \equiv w \equiv 2, 17, 26, 41, \text{or } 50 \pmod{60}$, and so on. Compiling all this data, we also have found that there are no nontrivial perfect codes in $J(2w - r, w)$ and $J(2w + r, w)$ for all $1 \leq r \leq 14$ with possible exceptions for $r = 6, 9, \text{and } 12$. This comes together with modulos conditions imposed on $w$ and $n - w$ for any $e$-perfect code in $J(n, w)$. Assume $N$ is partitioned into two subsets $A$ and $B$, such that $|A| = w$, $|B| = n - w$, and the vector of the $(w, 0)$ configuration is a codeword. By considering the way in which the vectors of the configuration $(w - e - 2, e + 2)$ are J-covered we can get some more divisibility conditions that rule out some of the combinations between $w$ and $n - w$. We can proceed to get more divisibility conditions. But no other Johnson graph $J(n, w)$ was ruled out as a candidate to contain nontrivial perfect codes. Similarly, other results can be obtained from the configuration distribution, but the outcome is less significant.

From the proof of Theorem 3.1 we can see the involved structure of e-perfect codes in $J(n, w)$. If we partition $N$ into two subsets $A$ and $B$, such that $|A| = w$ and $|B| = n - w$ and the vector of the $(w, 0)$ configuration is a codeword, then in the codewords of configuration $(w - e - 2, 2e + 1)$ we have in the $A$ part a complement of a Steiner system $S(e + 1, 2e + 1, w)$ for each set of codewords which C-cover any fixed $e + 1$ positions of $B$. Similarly, we can obtain (and this can be an alternative proof for Corollary 3.2) that in the $B$ part there is a Steiner system $S(e + 1, 2e + 1, n - w)$ for each set of codewords for which the complements C-cover any fixed $e + 1$ positions in $A$. This involved structure, together with the Steiner system of Theorem 3.3 and Corollary 3.4, seems to be impossible to achieve. This is without taking into consideration all the other configurations which are becoming more and more complicated. Hence, we
get more confidence in the belief in the conjecture that no nontrivial perfect codes exist in the Johnson scheme.

Acknowledgment. The author would like to thank Prof. Chris Mitchell for his hospitality in Royal Holloway College, which made it possible to obtain these results.

REFERENCES