Triple systems for identifying quadruples

Iiro Honkala[*]

Department of Mathematics
University of Turku
20014 Turku, Finland
e-mail: honkala@utu.fi

Abstract

A collection C of distinct 3-element subsets of the set $S = \{1, 2, \ldots, n\}$ is called an identifying system of the quadruples of S, if every 4-element subset of S contains at least one of the triples in C, and moreover, no two 4-element subsets of S contain exactly the same triples of C. We consider the minimal possible cardinality of such a system, and show, in particular, that for $n = 6, 7$ and 8, the minimal cardinalities are 8, 14 and 26, respectively.

1 Introduction and basics

We consider the problem of identifying m-tuples by k-tuples from [8].

Definition 1 *A collection C of distinct k-element subsets of $S = \{1, 2, \ldots, n\}$ is called a* system of k-tuples identifying the m-tuples of S, *where $k < m$, if every m-element subset of S contains at least one of the k-tuples in C, and moreover, no two m-element subsets of S contain exactly the same k-tuples of C. The k-tuples in C are called* blocks. *The minimum cardinality of such a system is denoted by $W(n, k, m)$.*

In this paper we only consider triple systems identifying the quadruples of S, i.e., the case $k = 3$, $m = 4$, and show that the minimum cardinalities in such triple systems for $n = 4, 5, 6, 7, 8$ are $1, 4, 8, 14, 26$.

It is often convenient to use the expression that a quadruple *gets a vote* from a triple if the triple is contained in the quadruple.

It is often convenient to illustrate the triples by their incidence vectors: the incidence vector of the triple $\{h, i, j\}$ is the binary vector of length n with 1's in coordinates h, i and j, and zeros elsewhere. Our problem is in this way related to

[*] Research supported by the Academy of Finland under grant 44002.

the following problem in coding theory. Denote by $\mathbb{F}_2$ the binary alphabet $\{0,1\}$ and by $d(\mathbf{x},\mathbf{y})$ the Hamming distance between $\mathbf{x}$ and $\mathbf{y}$, i.e., the number of coordinates in which $\mathbf{x}$ and $\mathbf{y}$ disagree. The number of 1's in $\mathbf{x}$ is called the weight of $\mathbf{x}$. Any nonempty subset C of $\mathbb{F}_2^n$ is called a binary code of length n. Karpovsky, Chakrabarty and Levitin [9] consider the following set-up: Assume that 2^n processors are arranged in the nodes of the binary n-dimensional hypercube. Any chosen processor can check itself and all the nodes within Hamming distance r, and reports YES if no problems are detected and NO, otherwise. We want to have a code C consisting of some of the nodes in the hypercube such that when those processors are chosen and perform the checking process described, then based on the YES/NO answers — assuming that at most one of the processors in the hypercube is malfunctioning — we can uniquely identify the malfunctioning processor, or know that everything is fine. In other words, we consider codes that satisfy the following definition, where

$$B_r(\mathbf{x}) = \{\mathbf{y} \in \mathbb{F}_2^n \mid d(\mathbf{y},\mathbf{x}) \le r\}.$$

Definition 2 *A binary code C of length n is called r-identifying (where $r < n$) if the sets $B_r(\mathbf{x}) \cap C$, $\mathbf{x} \in \mathbb{F}_2^n$, are nonempty and different.*

For this problem, we also refer to [1], [2], [7], [8], [10], [11], [12]. Instead of the binary hypercubes, the same problem can be considered for other graphs, see, e.g., [9], [3], [4], [5].

Our topic is a corresponding problem for constant weight codes, where all the codewords have the same weight. The case $k = 2$, $m = 3$ has been used in constructing identifying codes and amounts to finding a subgraph of the complete graph K_n with girth at least 5 and as many edges as possible; see [8].

Let $S = \{1,2,\ldots,n\}$. A permutation σ of the set S is called an automorphism of C if $C = \{\{\sigma(h),\sigma(i),\sigma(j)\} : \{h,i,j\} \in C\}$. A system of triples identifying the quadruples of S is called *cyclic*, if it has $\sigma = (123\ldots n)$ as an automorphism. If a is any subset of S, we call all the sets $\sigma^i(a)$, $i = 1,2,\ldots,n$, its *conjugates.* Of course, a conjugacy class, consisting of a set and its conjugates, may contain fewer than n sets.

Our topic is related to the Turan problem, cf., e.g., [6], in which it is required that every m-tuple contains at least one of the k-tuples in the system.

Theorem 1

$$\frac{n(n-1)(n-3)}{12} \le W(n,3,4) \le \begin{cases} \frac{n(7n^2-27n+18)}{54} & \textit{if } n \equiv 0 \pmod 3 \\ \frac{(n-1)(7n^2-20n+4)}{54} & \textit{if } n \equiv 1 \pmod 3 \\ \frac{(n-2)(7n^2-13n-2)}{54} & \textit{if } n \equiv 2 \pmod 3. \end{cases}$$

Proof Assume that C is a system of K triples identifying the quadruples of the set $S = \{1,2,\ldots,n\}$. There can be at most K quadruples that only get one vote, and all the others need at least two. Each triple gives $n-3$ votes and therefore

$$K \cdot 1 + \left(\binom{n}{4} - K\right) \cdot 2 \le K \cdot (n-3),$$

giving the lower bound.

Take as blocks all the triples $\{h, i, j\}$ such that at least two of h, i and j are congruent modulo 3 (cf., e.g., [6, p. 260]). We are taking all the triples except $n^3/27$ if $n \equiv 0 \pmod 3$, $(n-1)^2(n+2)/27$ if $n \equiv 1 \pmod 3$ and $(n-2)(n+1)^2/27$ if $n \equiv 2 \pmod 3$.

Given any quadruple, $\{g, h, i, j\}$, at least two of its elements, say g and h are congruent modulo 3, and then $\{g, h, i\}$ and $\{g, h, j\}$ are blocks. A quadruple is uniquely determined by any two triples voting for it. □

2 The cases $n = 4, 5, 6, 7$

The case $n = 4$ is of course trivial: any nonempty subset of the triples identifies the unique quadruple. The case $n = 5$ is also easy to deal with.

Theorem 2 *The smallest system of triples identifying the quadruples of the set $S = \{1, 2, 3, 4, 5\}$ has four blocks.*

In fact, there are three essentially different such systems. After a suitable permutation of the elements of S the system is as in one of the following arrays:

$$\begin{array}{ccccc} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{array} \quad \begin{array}{ccccc} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{array} \quad \begin{array}{ccccc} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1. \end{array}$$

This is in fact evident: a quadruple not containing an element i gets a vote from all the rows of the array with 0 in the i-th column and only from them; therefore each column must contain at least one 0, and all the columns must be different. The fact that each row must contain exactly two 0's leaves only the above three possibilities, with four, three and two columns with only a single 0, respectively. The lower bound follows from Theorem 1.

Theorem 3 *The smallest system of triples identifying the quadruples of $S = \{1, 2, 3, 4, 5, 6\}$ has eight blocks. Apart from a permutation of the elements of S, such a system is unique, and can be made cyclic.*

Proof By Theorem 1, at least eight blocks are needed.

One easily checks that the cyclic system $\{1, 3, 5\}$, $\{2, 4, 6\}$, $\{1, 2, 4\}$, $\{2, 3, 5\}$, $\{3, 4, 6\}$, $\{4, 5, 1\}$, $\{5, 6, 2\}$, $\{6, 1, 3\}$ is as required (the verification can be found in Figure 1).

We need to prove the uniqueness. Assume that C is a system of triples identifying the quadruples of S and that C has eight blocks.

1) Every element of S is contained in exactly four triples of C: otherwise, since all in all the elements of S appear 24 times in C, there is an element i of S which is contained in more than four blocks, and the three or fewer blocks not containing i should identify all the 4-subsets of $S \setminus \{i\}$, which is not possible by Theorem 2.

2) Every pair $\{i,j\}$, $i \neq j$, of elements of S must be contained in at least one block: otherwise each triple contains either i or j (since i appears in exactly four triples and so does j), and consequently the quadruple $S \setminus \{i,j\}$ cannot contain any of them.

3) No pair $\{i,j\}$, $i \neq j$, of elements of S is contained in four blocks: otherwise, if $u,v,w \in S \setminus \{i,j\}$, then the quadruples $\{u,v,w,i\}$ and $\{u,v,w,j\}$ cannot be separated.

4) No pair $\{i,j\}$, $i \neq j$, of elements of S, is contained in three blocks: Assume without loss of generality that $i=1$, $j=2$, and that $\{1,2,3\}$, $\{1,2,4\}$, $\{1,2,5\}$ are in C. The one remaining triple that contains 1 and the one remaining triple that contains 2 must both contain the element 6; otherwise (since 6 is anyway contained in exactly four blocks) the pair $\{1,6\}$ or $\{2,6\}$ does not belong to any block, contrary to 2). But now the quadruples $\{1,3,4,5\}$ and $\{2,3,4,5\}$ cannot be separated.

A trivial counting argument now shows that there is a pair, say $\{1,2\}$, which is contained in a unique block, and since every element of S is contained in exactly four blocks, there is a block, say $\{4,5,6\}$ which contains neither 1 nor 2. By 3) and 4), we can threrefore assume that the incidence vectors look like

$$\begin{array}{cccccc}
1 & 1 & 0 & & & \\
1 & 0 & 1 & & & \\
1 & 0 & 1 & & & \\
1 & 0 & 0 & & & \\
0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & & & 1 \\
0 & 0 & 0 & 1 & 1 & 1
\end{array}$$

where the last bit of the seventh row follows by applying 4) to the pair $\{1,6\}$.

By symmetry, we can assume that 4 belongs to the seventh block and 5 does not. Then using 4) to $\{2,4\}$ we see that 4 does not belong to the first block, and using 4) to $\{4,6\}$ we see that 5 belongs to the fourth block, resulting in the array:

$$\begin{array}{cccccc}
1 & 1 & 0 & 0 & & \\
1 & 0 & 1 & & & \\
1 & 0 & 1 & & & \\
1 & 0 & 0 & & 1 & \\
0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1.
\end{array}$$

If now 4 belongs to the fourth block, we see that apart from the order of the second and third rows there is a unique way of completing the array, which becomes

$$\begin{array}{cccccc}
1 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1.
\end{array}$$

By swapping the first and fifth columns, and the second and sixth, we get our earlier cyclic system

$$\begin{array}{cccccc}
0 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 0.
\end{array}$$

Assuming that 4 does not belong to the fourth block, we can complete the fourth row and by symmetry also the fourth column (changing the roles of the second and third block if necessary) as in the array below, and then the second row. Now the remaining element of the first block is 5 and the remaining element of the third block is 6, or the other way round. Applying 2) to $\{3, 6\}$, we exclude the latter possibility, and therefore C must be

$$\begin{array}{cccccc}
1 & 1 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1.
\end{array}$$

Rewriting the columns in the order 3, 6, 2, 1, 4, 5 again gives our original cyclic system. □

Using the uniqueness part of the previous result we now get the uniqueness in the case $n = 7$ almost for free!

We first construct a cyclic system with 14 blocks that identifies the quadruples of the set $\{1, 2, \ldots, 7\}$: Take as the blocks $\{1, 2, 4\}$ and $\{1, 3, 4\}$ and all their cyclic shifts. Using the incidence vectors, we take the conjugacy classes A and B represented by

$$\begin{array}{ccccccc|c}
\hline
1 & 1 & 0 & 1 & 0 & 0 & 0 & A \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & B \\
\hline
\end{array}$$

and the following array shows how the members of the conjugacy classes of the quadruples get votes from the conjugacy classes of the blocks:

1	1	1	1	0	0	0	AB
1	1	1	0	1	0	0	A
1	1	1	0	0	1	0	B
1	1	0	1	1	0	0	AB
1	1	0	1	0	1	0	AB

Since any two votes always uniquely identify the quadruple, we see that these 14 blocks form the required system.

Theorem 4 *The smallest number of blocks in a system of triples identifying the quadruples of* $S = \{1, 2, 3, 4, 5, 6, 7\}$ *is* 14*. Apart from a permutation of the elements of* S*, such a system is unique, and can be made cyclic.*

Proof By Theorem 1, at least 14 blocks are required. We have already constructed such a system. It suffices to prove the uniqueness.

By Theorem 3, every element of S appears in exactly six blocks. We can assume that the blocks that do not contain the element 7 are as in Figure 1. Denote this subset of eight blocks by D. From Figure 1 we see that there is a set U of 12 quadruples which do not get any votes from D, together requiring at least $6 \cdot 1 + 6 \cdot 2 = 18$ votes, by the standard counting argument.

The 6-cycle $\tau = (123456)$ is an automorphism of D. Since the pair $\{1, 2\}$ is contained in a unique block of D, and $\{1, 3\}$ and $\{1, 4\}$ are contained in two each, we can immediately deduce that all the six pairs $\{1, 2\}$, $\{2, 3\}$, $\{3, 4\}$, $\{4, 5\}$, $\{5, 6\}$, $\{6, 1\}$ are contained in a unique block of D; any other 2-subset of $S = \{1, 2, \ldots, 6\}$ is contained in exactly two blocks of D. Therefore $\{7, 1, 2\}$, $\{7, 2, 3\}$, $\ldots$, $\{7, 6, 1\}$ give three votes to the quadruples of U, whereas any other triple containing 7 only gives two votes. The only possibility is therefore to take the six triples which give three votes each. □

Of course, the system given in Figure 1 is the same as our cyclic system constructed previously, after a suitable permutation of the elements of S. In particular, there is a 7-cycle τ', which is an automorphism of the system.

3 The case $n = 8$

The nice structure of the unique system in the case $n = 7$ was quite special. Indeed, we can prove more:

Theorem 5 *If* C *is a system of* 15 *triples identifying the quadruples of* $S = \{1, 2, \ldots, 7\}$*, then after a suitable permutation of the elements of* S*,* C *consists of the* 14 *blocks of Figure 1 together with an arbitrary* 15*-th block.*

Moreover, if we know that C *contains the eight triples in Figure 1 not containing* 7*, together with seven triples containing* 7*, then* C *contains all the* 14 *blocks in Figure 1.*

Proof As $15 \cdot 3 \geq 7 \cdot 6$, there is an element of S that appears in at least seven blocks. By Theorem 3, no element can appear in more than seven blocks, and we can therefore without loss of generality assume that the element 7 appears in exactly seven blocks. The eight blocks not containing 7 identify the quadruples contained in $\{1,2,3,4,5,6\}$, and by Theorem 3, we can assume that after a suitable permutation of S, the blocks not containing the element 7 are the blocks *a*–*h* in Figure 1. The set D consisting of these eight blocks has $\tau = (123456)$ as an automorphism. We use the same argument as in the previous proof, and denote by P the set consisting of $\{1,2\}$, $\{2,3\}$, $\{3,4\}$, $\{4,5\}$, $\{5,6\}$, $\{6,1\}$ and by $\overline{P}$ the set of triples $\{i,j,7\}$ for which $\{i,j\} \in P$.

The remaining blocks in C do not give any more votes to the quadruples that do not contain 7: of 15 such quadruples, nine get two votes, and six get just one (namely from *c*–*h*) as we see from Figure 1. Of the 20 quadruples containing the element 7, the sets $\{1,3,5,7\}$ and $\{2,4,6,7\}$ have already been taken care of, since $\{1,3,5,7\}$ (resp. $\{2,4,6,7\}$) is the only quadruple whose only vote comes from $a = \{1,3,5\}$ (resp. $b = \{2,4,6\}$). The six quadruples $\{1,2,4,7\}$, $\{2,3,5,7\}$, …, $\{1,3,6,7\}$ (also of the form $\{h,i,j\} \cup \{7\}$, $\{h,i,j\} \in D$) simply need one more vote each.

Of the 20 quadruples containing the element 7, twelve get no votes from D. They must together get at least $7 \cdot 1 + 5 \cdot 2 = 17$ votes, because there are only seven blocks in $C \setminus D$. From the previous proof we know that a triple $\{7,i,j\}$ contributes three votes if and only if $\{i,j\} \in P$; all the other triples only contribute two votes. Consequently, at least three of the triples in $C \setminus D$ must belong to $\overline{P}$.

Assume first that there are *exactly* three elements of $\overline{P}$ in $C \setminus D$. In this case, since $3 \cdot 3 + 4 \cdot 2 = 17$, there are no extra votes, and therefore each of the 12 quadruples that did not get any votes from D gets one or two votes. Using the automorphism τ it suffices to check the following four cases.

Case 1 $C \cap \overline{P} = \{\{1,2,7\},\{2,3,7\},\{3,4,7\}\}$: The quadruples $\{4,5,6,7\}$ and $\{5,6,7,1\}$ have no votes so far. Since neither $\{4,5,7\}$ nor $\{5,6,7\}$ belongs to C (and of course $\{4,5,6\} \notin C$), we conclude that $\{4,6,7\}$ — and similarly $\{5,7,1\}$ — must be in C. The quadruples $\{2,4,5,7\}$ and $\{3,5,6,7\}$ have no votes yet and $\{1,3,6,7\}$ still requires one more vote. Hence one of the remaining two blocks in C must give a vote to at least two of them. This is only possible using the triple $\{3,6,7\}$, which must therefore belong to C. The quadruple $\{2,4,5,7\}$ is still without votes, and $\{2,5,6,7\}$ needs one more, and hence $\{2,5,7\}$ must be the last remaining triple in C. But the constructed system C does not have the required property, e.g., $\{3,4,5,7\}$ and $\{1,3,4,7\}$ both have received just one vote and both of them from $\{3,4,7\}$.

Case 2 $C \cap \overline{P} = \{\{1,2,7\},\{2,3,7\},\{4,5,7\}\}$: We immediately see that $\{1,5,7\} \in C$, because $\{1,5,6,7\}$ must get a vote from it. The quadruple $\{1,3,4,7\}$ has no votes yet, and of course $\{3,4,7\} \notin C$. However, if $\{1,3,7\} \in C$, then one of the 12 quadruples that did not get any votes from D, namely $\{1,2,3,7\}$ already gets three votes, which cannot be the case. Consequently, $\{1,4,7\} \in C$ and this is the only vote $\{1,3,4,7\}$ gets. Consequently, $\{1,4,6,7\}$ must get one more vote from the two remaining blocks. Since $\{1,6,7\}$ is not in C, $\{4,6,7\}$ must be. But now there is no quadruple among the twelve which would only be voted by $\{4,6,7\}$, and hence we

The blocks

1	0	1	0	1	0	0	a
0	1	0	1	0	1	0	b
1	1	0	1	0	0	0	c
0	1	1	0	1	0	0	d
0	0	1	1	0	1	0	e
1	0	0	1	1	0	0	f
0	1	0	0	1	1	0	g
1	0	1	0	0	1	0	h
1	1	0	0	0	0	1	α
0	1	1	0	0	0	1	β
0	0	1	1	0	0	1	γ
0	0	0	1	1	0	1	δ
0	0	0	0	1	1	1	ϵ
1	0	0	0	0	1	1	ζ

The quadruples and their votes

0	0	0	1	1	1	1		$\delta\epsilon$
0	0	1	0	1	1	1		ϵ
0	1	0	0	1	1	1	g	ϵ
1	0	0	0	1	1	1		$\epsilon\zeta$
0	0	1	1	0	1	1	e	γ
0	1	0	1	0	1	1	b	
1	0	0	1	0	1	1		ζ
0	1	1	0	0	1	1		β
1	0	1	0	0	1	1	h	ζ
1	1	0	0	0	1	1		$\alpha\zeta$
0	0	1	1	1	0	1		$\gamma\delta$
0	1	0	1	1	0	1		δ
1	0	0	1	1	0	1	f	δ
0	1	1	0	1	0	1	d	β
1	0	1	0	1	0	1	a	
1	1	0	0	1	0	1		α
0	1	1	1	0	0	1		$\beta\gamma$
1	0	1	1	0	0	1		γ
1	1	0	1	0	0	1	c	α
1	1	1	0	0	0	1		$\alpha\beta$
0	0	1	1	1	1	0	e	
0	1	0	1	1	1	0	bg	
1	0	0	1	1	1	0	f	
0	1	1	0	1	1	0	dg	
1	0	1	0	1	1	0	ah	
1	1	0	0	1	1	0	g	
0	1	1	1	0	1	0	be	
1	0	1	1	0	1	0	eh	
1	1	0	1	0	1	0	bc	
1	1	1	0	0	1	0	h	
0	1	1	1	1	0	0	d	
1	0	1	1	1	0	0	af	
1	1	0	1	1	0	0	cf	
1	1	1	0	1	0	0	ad	
1	1	1	1	0	0	0	c	

Figure 1: The unique minimal system in the case $n = 7$.

would again require at least 18 votes instead of 17.

Case 3 $C \cap \overline{P} = \{\{1,2,7\},\{2,3,7\},\{5,6,7\}\}$: Now $\{3,4,5,7\}$ needs a vote, and therefore $\{3,5,7\} \in C$. The quadruple $\{1,3,4,7\}$ has no votes yet, and we conclude that $\{1,4,7\} \in C$ (again, $\{1,3,7\} \in C$ implies that $\{1,2,3,7\}$ would get three votes); and $\{1,3,4,7\}$ gets its only vote from $\{1,4,7\}$. Consequently, $\{1,4,6,7\}$ must get another vote, and it must come from $\{4,6,7\}$. But now none of our 12 words gets just one vote and that from $\{4,6,7\}$; consequently, at least 18 votes would again be required.

Case 4 $C \cap \overline{P} = \{\{1,2,7\},\{3,4,7\},\{5,6,7\}\}$: Among the 12 quadruples, only three have not received any votes. Consequently, at least one of the remaining four blocks in C has the property that there is no quadruple among the 12 which would only get a vote from it.

Assume then that there are four triples of $\overline{P}$ in $C \setminus D$. Using τ, it suffices to check the following three cases.

Case 5 $C \cap \overline{P} = \{\{1,2,7\},\{2,3,7\},\{3,4,7\},\{4,5,7\}\}$: We see that the quadruple $\{1,5,6,7\}$ must get a vote from $\{1,5,7\} \in C$. Now $\{3,5,6,7\}$, $\{1,4,6,7\}$, $\{2,5,6,7\}$, $\{1,3,6,7\}$ all need at least one more vote. A triple gives a vote to two of them only if the triple contains 6 together with 1, 3 or 5 (no triple gives a vote to more than two of them), which implies that $\{1,6,7\}$ or $\{5,6,7\}$, which both belong to $\overline{P}$, should be a block, which is not the case.

Case 6 $C \cap \overline{P} = \{\{1,2,7\},\{2,3,7\},\{3,4,7\},\{5,6,7\}\}$: Now $\{4,5,6,7\}$ and $\{1,5,6,7\}$ have only one vote so far, namely from $\{5,6,7\}$. One of them must get a second vote, and so $\{4,6,7\} \in C$ or $\{1,5,7\} \in C$. If $\{4,6,7\} \in C$, then the remaining two blocks in C should give at least one more vote to each of the quadruples $\{2,4,5,7\}$, $\{1,4,5,7\}$ and $\{1,3,6,7\}$, which is not possible because $\{4,5,7\} \notin C$. In the same way, if $\{1,5,7\} \in C$, then the remaining two blocks in C should give at least one vote to each of the quadruples $\{2,4,5,7\}$, $\{1,4,6,7\}$ and $\{1,3,6,7\}$, which is not possible since $\{1,6,7\} \notin C$.

Case 7 $C \cap \overline{P} = \{\{1,2,7\},\{2,3,7\},\{4,5,7\},\{5,6,7\}\}$: The quadruples $\{3,4,6,7\}$ and $\{1,3,6,7\}$ need one more vote each. If $\{3,6,7\} \notin C$, then $\{1,3,7\} \in C$ and $\{4,6,7\} \in C$, but in this case $\{1,2,3,7\}$ and $\{4,5,6,7\}$ would already have three votes each, and our total number of votes, namely 18 by the words in $C \setminus D$ to the 12 quadruples is not enough. Hence $\{3,6,7\} \in C$. So far, $\{1,3,4,7\}$ and $\{1,4,6,7\}$ have no votes, and therefore both the remaining blocks in C must give a vote to at least one of them. Hence the remaining blocks are among $\{1,3,7\}$, $\{1,4,7\}$, $\{4,6,7\}$. But none of them can help to separate between $\{1,2,6,7\}$ and $\{1,2,5,7\}$, both so far being voted only by $\{1,2,7\}$.

Assume finally that there are five triples of $\overline{P}$ in $C \setminus D$.

Case 8 $C \cap \overline{P} = \{\{1,2,7\},\{2,3,7\},\{3,4,7\},\{4,5,7\},\{5,6,7\}\}$: At this stage, $\{1,4,6,7\}$ has no votes. Consequently, $\{1,4,7\} \in C$ or $\{4,6,7\} \in C$. In both cases, the last remaining block in C should give one more vote to $\{1,3,6,7\}$ and to either $\{1,2,6,7\}$ or $\{1,2,5,7\}$, which is impossible (because we know that $\{1,6,7\} \notin C$).□

If C is a system of 15 triples identifying the quadruples of $S = \{1,2,\dots,7\}$, then the "superfluous" triple is easy to find: by the previous theorem it is the triple

$\{i, j, k\}$ where i, j and k are the three elements of S that belong to exactly seven triples (all the other elements of S belong to exactly six).

Theorem 6 *Assume that C is a system of at most 15 triples identifying the quadruples of $\{1, 2, \ldots, 7\}$ and that C contains the eight blocks not containing 7 listed in Figure 1. Then C contains all the blocks in Figure 1.*

Proof In view of the previous proofs it suffices to consider the case where C contains the eight blocks not containing 7 in Figure 1 (the set of which we call D), one more triple x which does not contain the element 7, and six triples which contain the element 7.

Let $\overline{P}$ be as in the previous proof. There are at least 11 quadruples containing 7, which do not get any votes from the blocks not containing 7. The same counting argument as in the previous proof shows that at least four of the six blocks in C that contain 7 must belong to $\overline{P}$, and moreover, if there are exactly four elements of $\overline{P}$ in C, then there is a quadruple, whose only vote comes from x.

Using the permutation τ, we see that there are only four cases to check.

Case 1 $C \cap \overline{P} = \{\{1, 2, 7\}, \{2, 3, 7\}, \{3, 4, 7\}, \{4, 5, 7\}\}$: From Figure 1 we see that the quadruple $\{1, 5, 6, 7\}$ has no votes yet. Either $\{1, 5, 7\}$ is in C or $x = \{1, 5, 6\}$ (but not both).

Assume first that $\{1, 5, 7\}$ is in C. Then one of the quadruples $\{3, 5, 6, 7\}$ and $\{1, 4, 6, 7\}$ gets a vote from x and the other from the one remaining triple in C, which must belong to the set $A_1 = \{\{3, 5, 7\}, \{3, 6, 7\}, \{1, 4, 7\}, \{4, 6, 7\}\}$. To separate between $\{4, 5, 6, 7\}$ and $\{2, 4, 5, 7\}$, both only with the vote from $\{4, 5, 7\}$ so far, at least one of the triples in $A_2 = \{\{4, 6, 7\}, \{2, 4, 7\}, \{2, 5, 7\}\}$ must be in C. The remaining block must therefore be the only triple both in A_1 and A_2, namely $\{4, 6, 7\}$. Then $x = \{3, 5, 6\}$. The resulting C does not have the required property, though, because the quadruples $\{1, 2, 3, 6\}$ and $\{1, 3, 6, 7\}$ are both only voted by $\{1, 3, 6\}$.

Assume then that $x = \{1, 5, 6\}$. To separate between $\{1, 2, 6, 7\}$ and $\{1, 2, 5, 7\}$ (both only with a vote from $\{1, 2, 7\}$ so far), at least one of the triples in $B_1 = \{\{2, 6, 7\}, \{1, 5, 7\}, \{2, 5, 7\}\}$ must be in C. Because the quadruples $\{3, 5, 6, 7\}$ (resp. $\{1, 4, 6, 7\}$) have no votes yet, at least one triple in $B_2 = \{\{3, 5, 7\}, \{3, 6, 7\}\}$ (resp. $B_3 = \{\{1, 4, 7\}, \{4, 6, 7\}\}$) must be in C. However, B_1, B_2 and B_3 are disjoint, and we can only take two more triples to C.

Case 2 $C \cap \overline{P} = \{\{1, 2, 7\}, \{2, 3, 7\}, \{3, 4, 7\}, \{5, 6, 7\}\}$: We know that x must vote for either of the two quadruples $\{2, 4, 5, 7\}$ or $\{1, 4, 6, 7\}$ with no votes so far (and then $x = \{2, 4, 5\}$ or $\{1, 4, 6\}$ respectively), and the other one must be voted by a triple containing 7, and therefore one of the triples in the set $A_1 = \{\{2, 4, 7\}, \{2, 5, 7\}, \{1, 4, 7\}, \{4, 6, 7\}\}$ is in C. To separate between the quadruples $\{4, 5, 6, 7\}$ and $\{1, 5, 6, 7\}$ with both only the vote from $\{5, 6, 7\}$ so far, at least one triple in $A_2 = \{\{1, 5, 7\}, \{4, 6, 7\}\}$ is in C. To separate between $\{1, 2, 6, 7\}$ and $\{1, 2, 5, 7\}$, at least one triple in $A_3 = \{\{2, 6, 7\}, \{1, 5, 7\}, \{2, 5, 7\}\}$ is in C, and to separate between $\{1, 3, 4, 7\}$ and $\{3, 4, 5, 7\}$ at least one triple in $A_4 = \{\{1, 3, 7\}, \{1, 4, 7\}, \{3, 5, 7\}\}$ is in C. There are only two more blocks to choose. We cannot take $\{4, 6, 7\}$ from A_2, because $\{4, 6, 7\} \notin A_3$, $\{4, 6, 7\} \notin A_4$, and A_3 and A_4 are disjoint. Hence $\{1, 5, 7\}$ from

A_2 belongs to C. Because $\{1,5,7\} \notin A_1$, $\{1,5,7\} \notin A_4$, and $A_1 \cap A_4 = \{\{1,4,7\}\}$, the last block must be $\{1,4,7\}$. But now $\{4,5,6,7\}$ and $\{3,5,6,7\}$ only get a vote from $\{5,6,7\}$.

Case 3 $C \cap \overline{P} = \{\{1,2,7\},\{2,3,7\},\{4,5,7\},\{5,6,7\}\}$: We know that x must vote for either of the two quadruples $\{1,3,4,7\}$ and $\{1,4,6,7\}$ with no votes so far, i.e., $x = \{1,3,4\}$ or $x = \{1,4,6\}$, and the other quadruple must get a vote from a block containing 7. Therefore at least one triple in $A_1 = \{\{1,3,7\},\{4,6,7\}\}$ must be in C ($\{1,4,7\} \notin C$: otherwise there is no quadruple whose only vote comes from x). To separate between the quadruples $\{1,2,5,7\}$ and $\{1,2,6,7\}$ so far only voted by $\{1,2,7\}$, at least one triple in the set $A_2 = \{\{2,6,7\},\{1,5,7\},\{2,5,7\}\}$ must be in C. To separate between the quadruples $\{3,4,5,7\}$ and $\{2,4,5,7\}$ so far only voted by $\{4,5,7\}$, at least one triple in $A_3 = \{\{2,4,7\},\{2,5,7\},\{3,5,7\}\}$ must be in C. Finally, to separate between $\{2,3,6,7\}$ and $\{2,3,4,7\}$ with only the vote from $\{2,3,7\}$ so far, at least one of the triples in $A_4 = \{\{2,4,7\},\{2,6,7\},\{3,6,7\}\}$ is in C. Since A_1 and $A_2 \cup A_3 \cup A_4$ are disjoint, we could only make it, if $A_2 \cap A_3 \cap A_4 \neq \emptyset$, which is not the case.

Case 4 $C \cap \overline{P} = \{\{1,2,7\},\{2,3,7\},\{3,4,7\},\{4,5,7\},\{5,6,7\}\}$: Assume first that $x = \{1,4,6\}$. The last remaining triple should separate between $\{1,2,5,7\}$ and $\{1,2,6,7\}$ and simultaneously between $\{1,5,6,7\}$ and $\{3,5,6,7\}$, which is only possible if the triple is $\{1,5,7\}$. However, $\{1,3,6,7\}$ and $\{1,2,3,6\}$ then only get one vote, both from $\{1,3,6\}$.

Assume therefore that $x \neq \{1,4,6\}$. The quadruple $\{1,4,6,7\}$ has not votes yet, and therefore the last triple (other than x) must be $\{1,4,7\}$ or $\{4,6,7\}$. In either case, the unknown x should still separate between $\{1,5,6,7\}$ and $\{3,5,6,7\}$ and simultaneously between $\{1,2,5,7\}$ and $\{1,2,6,7\}$, which is impossible. □

Consider now the case $n = 8$. Take as the first 24 blocks the triples $\{1,2,3\}$, $\{1,2,5\}$, $\{1,3,6\}$ and their cyclic shifts. Using the incidence vectors, we take the conjugacy classes A, B and C represented by

1	1	1	0	0	0	0	0	A
1	1	0	0	1	0	0	0	B
1	0	1	0	0	1	0	0	C

and it is easy to verify that all the members of the conjugacy classes of the quadruples get votes from the conjugacy classes of the blocks as follows:

1	1	1	1	0	0	0	0	AA
1	1	1	0	1	0	0	0	AB
1	1	1	0	0	1	0	0	ABC
1	1	1	0	0	0	1	0	A
1	1	0	1	1	0	0	0	B
1	1	0	0	1	1	0	0	BB
1	1	0	1	0	1	0	0	C
1	1	0	0	1	0	1	0	BC
1	1	0	1	0	0	1	0	CC
1	0	1	0	1	0	1	0	

where AA means that each member of the conjugacy gets a vote from two members of the conjugacy class A. Since two votes uniquely identify the quadruple, we see that it only remains to take care of the two quadruples in the last conjugacy class, and by taking, for instance, $\{1, 3, 5\}$ and $\{2, 4, 6\}$, as blocks, we get a system, which clearly identifies all the quadruples of the set $\{1, 2, \ldots, 8\}$.

Of course, there is no cyclic system with 26 blocks, because each conjugacy class of the triples consists of exactly eight triples.

In fact, this is the best we can do.

Theorem 7 *The smallest system of triples identifying the quadruples of* $S = \{1, 2, \ldots, 8\}$ *contains* 26 *blocks.*

Proof Assume that C would be such a system with only 25 blocks. By Theorem 4, every element belongs to at most 11 blocks, and at least one element, say 8, belongs to at least $\lceil 25 \cdot 3/8 \rceil = 10$ blocks. Let E denote the set of blocks that contain 8 and D the set of blocks that do not.

Assume first that $|E| = 11$ and $|D| = 14$. Since $11 \cdot 2/7 > 3$, there is an element of $\{1, 2, \ldots, 7\}$ which belongs to at least four blocks of E. Without loss of generality, this element is 7. Since the blocks of D form the unique triple system identifying the quadruples of $\{1, 2, ..., 7\}$ we know that 1, 2, …, 7 belong to exactly six blocks of D, and the blocks not containing 7 form the unique system identifying the quadruples of $\{1, 2, \ldots, 6\}$, so without loss of generality these eight blocks are as in Figure 1, and by Theorem 6, the whole D is as in Figure 1. Now the blocks of C not containing 7 consist of at most seven blocks in E and eight blocks of D, and form a system of at most 15 triples identifying the quadruples of the set $\{1, 2, 3, 4, 5, 6, 8\}$: and by Theorem 6, $\{1, 2, 8\}$, $\{2, 3, 8\}$, $\{3, 4, 8\}$, $\{4, 5, 8\}$, $\{5, 6, 8\}$ and $\{6, 1, 8\}$ are all in E, and there is at most one more block in E that does not contain both 7 and 8. So far, the quadruples (cf. Figure 1) $\{1, 3, 5, 7\}$ and $\{1, 3, 5, 8\}$ only get a vote from $\{1, 3, 5\}$, and $\{2, 4, 6, 7\}$ and $\{2, 4, 6, 8\}$ only from $\{2, 4, 6\}$, and one block cannot separate both pairs (and the blocks containing both 7 and 8 do not help).

Assume therefore that $|E| = 10$ and $|D| = 15$. Without loss of generality, D contains the 14 blocks in Figure 1.

We first show that it is not possible that an element of $\{1, 2, \ldots, 7\}$ would belong to four or more blocks in E. Using the automorphism τ' if necessary, we could then assume 7 is an element which belongs to at least four blocks of E. The eight or nine blocks of D not containing 7 together with the at most six blocks of E not containing 7 must form the triple system identifying the quadruples of the set $\{1, 2, 3, 4, 5, 6, 8\}$. By Theorem 6, this implies that $\{1, 2, 8\}$, $\{2, 3, 8\}$, $\{3, 4, 8\}$, $\{4, 5, 8\}$, $\{5, 6, 8\}$ and $\{6, 1, 8\}$ are in E. But as in the previous case, the one remaining block of D is not enough: we cannot simultaneously separate between $\{1, 3, 5, 7\}$ and $\{1, 3, 5, 8\}$ and $\{2, 4, 6, 7\}$ and $\{2, 4, 6, 8\}$.

Hence every element of $\{1, 2, \ldots, 7\}$ belongs to at most three blocks in E; in other words, one of them belongs to two blocks and all the others to three. By using the automorphism τ' if necessary, we can simultaneously assume that 7 belongs to three blocks and that the fifteenth block in D contains 7. Again the seven blocks of E

not containing 7 include $\{1, 2, 8\}$, $\{2, 3, 8\}$, $\{3, 4, 8\}$, $\{4, 5, 8\}$, $\{5, 6, 8\}$ and $\{6, 1, 8\}$ by Theorem 6. This in turn means that the 22 blocks that do not contain *both* 7 and 8 only give votes to eight of the fifteen quadruples containing both 7 and 8, leaving seven such quadruples so far without votes. The remaining three blocks, say x, y, z (all containing both 7 and 8) are not enough: although the set $\{x, y, z\}$ has seven nonempty subsets, the whole set $\{x, y, z\}$ is not available, because a quadruple $\{7, 8, i, j\}$ can only get two votes from blocks of the form $\{7, 8, h\}$. □

From the construction, we see that had it been allowed that (at most) one of the quadruples gets no votes, 25 blocks would have been enough. This is the smallest possible number of triples in this case: such a system can always be made to satisfy our original definition by adding one suitable block. For $n = 7$, the answer would still be 14, as shown by the trivial counting argument.

Acknowledgment: The author would like to thank the referee for many useful comments.

References

[1] U. Blass, I. Honkala, S. Litsyn, Bounds on identifying codes, Discrete Mathematics, to appear.

[2] U. Blass, I. Honkala, S. Litsyn, On binary codes for identification, Journal of Combinatorial Designs 8 (2000), 151–156.

[3] I. Charon, O. Hudry, A. Lobstein, Identifying codes with small radius in some infinite regular graphs, Electronic Journal of Combinatorics, submitted.

[4] I. Charon, I. Honkala, O. Hudry, A. Lobstein, General bounds for identifying codes in some infinite regular graphs, Electronic Journal of Combinatorics, submitted.

[5] I. Charon, I. Honkala, O. Hudry, A. Lobstein, The minimum density of an identifying code in the king lattice, Discrete Mathematics, submitted.

[6] Z. Füredi, Turan type problems, in: Surveys in Combinatorics 1991 (ed. A. D. Keedwell), Cambridge University Press, Cambridge, 1991, pp. 253–300.

[7] I. Honkala, T. Laihonen, S. Ranto, On codes identifying sets of vertices in Hamming spaces, Designs, Codes and Cryptography, to appear.

[8] I. Honkala, T. Laihonen, S. Ranto, On strongly identifying codes, Discrete Mathematics, to appear.

[9] M. G. Karpovsky, K. Chakrabarty, L. B. Levitin, On a new class of codes for identifying vertices in graphs, IEEE Transactions on Information Theory 44 (1998), 599–611.

[10] T. Laihonen, Sequences of optimal identifying codes, IEEE Transactions on Information Theory, submitted.

[11] T. Laihonen, S. Ranto, Families of optimal codes for strong identification, Discrete Applied Mathematics, submitted.

[12] S. Ranto, I. Honkala, T. Laihonen, Two families of optimal identifying codes in binary Hamming spaces, IEEE Transactions on Information Theory, submitted.

(Received 16 Mar 2001)