ELSEVIER

Theoretical Computer Science 181 (1997) 337–345

Theoretical Computer Science

Small weight bases for Hamming codes[1]

John Tromp[a,*], Louxin Zhang[a], Ying Zhao[b]

[a] *Department of Computer Science, University of Waterloo, Waterloo, Ont., Canada N2L 3G1*
[b] *Department of Mathematics, Shanxi Teacher's University, Linfei, 041004 Shanxi, China*

Abstract

We present constructions of bases for a Hamming code having small *width* and *height*, i.e. number of 1s in each row and column in the corresponding matrix. Apart from being combinatorially interesting in their own right, these bases also lead to improved embeddings of a hypercube of cliques into a same-sized hypercube.

1. Introduction

Let $n = 2^k - 1$, $k \geqslant 2$, and let A_k be the k by n matrix over $GF(2)$ whose ith column, for $1 \leqslant i \leqslant n$, is the k-bit binary representation of i. For example,

$$A_3 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

We denote by C_k the nullspace of A_k, i.e. the set of n-vectors x with $A_k \cdot x = 0^k$. We are interested in finding a basis of the nullspace, C_k, of A_k, that has small *height* and *width*. The height of a set of vectors is defined as the maximum number of ones in any vector, while width is defined as the maximum over all n positions, of the number of vectors in the set having a 1 in that position. A basis of height h and width w is called a (h, w)-basis. The pair (h, w) is called the *weight*.

Low weight bases for the nullspace C_k have applications in coding theory [8], combinatorial designs [2], network embeddings [1, 6], and distributing resources in hypercube computers [10]. In fact, C_k is a one-error-correcting code which was first discovered by Hamming [5] for words of length $2^k - k - 1$. More precisely, Hamming proved that the words of length $2^k - k - 1$ can be encoded as words of length $2^k - 1$ so that each word has Hamming distance at most 1 to exactly one codeword.

[1] This work was supported in part by an NSERC International Fellowship and ITRC.
* Correspondence address: CWI, P.O. Box 94079, 1090 GB Amsterdam, The Netherlands. E-mail: tromp@cwi.nl.

PII S0304-3975(96)00278-2

Recently, bases for C_k were shown to be useful for hypercube embeddings. An embedding of a network G into a network H consists of an assignment of nodes of G to nodes of H and a mapping from edges of G onto paths in H. Desirable properties of an embedding are small load (maximum number of nodes of G assigned to the same node in H), low dilation (maximum length of a path that an edge is mapped to) and low congestion (maximum number of paths using an edge). In [1], Aiello and Leighton discovered that for any $k > 0$, a (h,w)-basis for C_k induces a one-to-one embedding of a hypercube of cliques $H_{2^k-k} \otimes K_k$ in a same-sized hypercube H_{2^k} with dilation h and congestion $2w+2$. Moreover, this embedding is useful in finding efficient embeddings of (dynamic) binary trees in the hypercube and reconfigurations of the hypercube around faults.

Although the existence of a height 3 basis for C_k is well known, the existence question for a $(3,3)$-basis is open ([6, p. 430]). Towards this problem, only weak results were obtained in [1, 6, 9, 12]. In this paper, we present two classes of bases with small weight, which improve the existing bounds on weight. In Section 2, we present a $(3,5)$-basis for C_k that has a very simple structure.

There are many constructions of codes from the incidence matrices of graphs, designs, etc. (for example, see [3, 9]). Using the approach observed in [9], we construct a class of $(3,4)$-bases in Section 3. As a consequence, we obtain a better one-to-one embedding of a hypercube of cliques into a same-sized hypercube, with dilation 3 and congestion 10.

Finally, we propose a construction of $(3,3)$-bases. In [1], Aiello and Leighton observed that a primitive trinomial of degree k induces a $(3,3)$-basis for C_k. But, primitive trinomials do not always exist. This observation is generalized in Section 4. We show that the existence of a trinomial $f(x)$ such that $\gcd(f(x), x^{2^k-1}+1)$ is primitive of degree k implies a $(3,3)$-basis for C_k. We present results of computations supporting our conjecture that such trinomials always exist.

2. A simple construction of a (3, 5)-basis

Note that the rank of A_k equals k. It follows that C_k has rank $n-k$, and that a basis for it consists of $n-k$ linearly independent vectors. We identify a boolean n-vector with its *support*, i.e. the set of positions (as non-zero boolean k-vectors) where it has a 1. For example, the support of (0100101) is $\{010, 101, 111\}$. The product $A_k \cdot \{u, v, w\}$ is easily seen to equal the sum over GF(2) (bitwise exclusive-or) of u, v, and w. E.g. $A_3 \cdot \{010, 101, 111\} = 010 \oplus 101 \oplus 111 = 0^3$. To better visualize the exclusive-or operation, we sometimes write the vectors in the support below each other with the bits aligned:

$$\left\{\begin{matrix} 0 & 1 & 0, \\ 1 & 0 & 1, \\ 1 & 1 & 1 \end{matrix}\right\}.$$

For a bit b, we denote by $\overline{b}$ its complement $b \oplus 1$. For a binary string/vector x, $|x|$ denotes the length of x.

A basis of C_k is constructed as follows. For $x \in \{0,1\}^i$, and $i+p+2 \leqslant k$, let $b_{x,p}$ be the vector

$$\left\{\begin{array}{lllllllll} 0^{k-i-p-2} & 1 & x_1 & x_2 & \dots & x_{i-1} & x_i & 1 & 0^p, \\ 0^{k-i-p-2} & 0 & 1 & x_1 & \dots & x_{i-2} & \overline{x_i} & 1 & 0^p, \\ 0^{k-i-p-2} & 1 & \overline{x_1} & x_{1,2} & \dots & x_{i-2,i-1} & 1 & 0 & 0^p \end{array}\right\},$$

where we write $x_{i,j}$ for $x_i \oplus x_j$. For definiteness, we have for the cases $i = 0, 1$:

$$b_{\varepsilon,p} = \left\{\begin{array}{llll} 0^{k-p-2} & 1 & 1 & 0^p, \\ 0^{k-p-2} & 0 & 1 & 0^p, \\ 0^{k-p-2} & 1 & 0 & 0^p \end{array}\right\}, \qquad b_{x_1,p} = \left\{\begin{array}{lllll} 0^{k-p-3} & 1 & x_1 & 1 & 0^p, \\ 0^{k-p-3} & 0 & \overline{x_1} & 1 & 0^p, \\ 0^{k-p-3} & 1 & 1 & 0 & 0^p \end{array}\right\}.$$

Note that $A_k \cdot b_{x,p} = 0^k$, so that any $b_{x,p}$ is in C_k.

Our proposed basis simply consists of the set B of all $b_{x,p}$. We must check that these vectors are indeed independent and that we have the right number of them.

To see the latter, partition B into $k-1$ sets B_p, and each B_p into $k-p-1$ sets $B_{p,i}$, containing all $b_{x,p}$ with $|x| = i$. Clearly, different pairs (x,p) define different vectors. Thus, the size of B is

$$\sum_{p=0}^{k-2} \sum_{i=0}^{k-2-p} 2^i = \sum_{p=0}^{k-2} (2^{k-1-p} - 1) = 2^k - 2 - (k-1) = n - k.$$

Thus, to prove that B is a basis, it remains to show that its elements are linearly independent.

2.1. *Independence*

Consider any nonempty subset C of B. We prove independence by showing that the sum of all vectors in C is not 0^k.

Let p be minimal such that $C \cap B_p \neq \emptyset$ and for this p, let i be maximal such that $C \cap B_{p,i} \neq \emptyset$, say $b_{x,p} \in C \cap B_{p,i}$. By definition, $b_{x,p}$ has $0^{k-i-p-2}1x10^p$ in its support. For any other $b_{x',p'}$ to have $0^{k-i-p-2}1x10^p$ in its support, would require either $p' = p-1$ or $|x'| = |x|+1$, so by minimality of p and maximality of i, such a $b_{x',p'}$ cannot be in C. Since $b_{x,p}$ is thus the only vector in C with $0^{k-i-p-2}1x10^p$ in its support, the sum of all vectors in C also has $0^{k-i-p-2}1x10^p$ in its support and hence is not 0^k.

2.2. *Height and width*

The height of B is obviously 3, since each vector $b_{x,p}$ has exactly 3 one bits. We claim that the width of B is at most 5. To see this, consider any position z. If z is of the form $0^{k-q-1}10^q$ then it appears only in the support of $b_{\varepsilon,q}$, $b_{\varepsilon,q-1}$ (if $q > 0$), and $b_{1,q}$. Hence, the width at such positions is no more than 3.

Otherwise, z is of the form $0^{k-j-q-2}1y_1y_2\dots y_j10^q$. Consider the $b_{x,p}$ that have this z in their support. We necessarily have one of the following three cases.

1. $z = 1x10^p$. This implies $p = q$ and $x = y$, and so accounts for one $b_{x,p}$.
2. $z = 1x_1\dots x_{i-2}\overline{x_i}10^p$. This implies $p = q$, $x_{1:i-2} = y_{1:j-1}$ and $x_i = \overline{y_j}$, and so accounts for two $b_{x,p}$ (x_{i-1} can be 0 or 1).
3. $z = 1\overline{x_1}x_{1,2}\dots x_{i-2,i-1}100^p$. This implies $p = q - 1$ and $x_1 = \overline{y_1}, x_2 = y_2 \oplus x_1 = \overline{y_1} \oplus y_2, x_3 = y_3 \oplus x_2 = \overline{y_1} \oplus y_2 \oplus y_3, \dots, x_{i-1} = \overline{y_1} \oplus y_2 \oplus \dots \oplus y_j$, and so accounts for two $b_{x,p}$ (x_i can be 0 or 1).

In total we find that at most five $b_{x,p}$ can have a one in position z, as claimed.

3. A (3, 4) basis

While the (3,5) basis may be preferred in some applications for its simplicity, we can get a better (3,4) basis by combining results from finite fields with an inductive construction based on finding Hamiltonian paths in complete bipartite graphs.

We start with the empty base B_1 for the null space $C_1 = \{0\}$ of A_1, which is the 1 by 1 matrix (1). Next we explain how to extend B_k to a basis B_{k+1} for the null space C_{k+1}. A subset B'_k of $2^k - 1 - k$ vectors in B_{k+1} will be derived from the $2^k - 1 - k$ vectors in B_k. Namely, for each vector $\{u, v, w\}$ in B_k, where $u, v, w \in \{0,1\}^k$, we put $\{0u, 0v, 0w\}$ into B'_k.

We form B_{k+1} as the union of B'_k and a set B of $2^k - 1$ more vectors, to get the required number of $2^k - 1 - k + 2^k - 1 = 2^{k+1} - 1 - (k+1)$ vectors. These vectors will have a support consisting of one position in $X = 01\{0,1\}^{k-1}$ and one in each $Y_i = 1i\{0,1\}^{k-1}$, $i = 0, 1$. Note that, for such a vector $\{01x, 10y_0, 11y_1\}$ to be in the nullspace, it must satisfy $x = y_0 \oplus y_1$, so that it is determined by just the pair $(10y_0, 11y_1) \in Y_0 \times Y_1$. Our problem can thus be seen as the selection of $2^k - 1$ edges in the complete bipartite graph G on $Y_0 \cup Y_1$. We will consider X to be a set of colors and say that an edge between $10y_0$ and $11y_1$ has *color* $01(y_0 \oplus y_1) \in X$. Getting a low width basis corresponds to minimizing the maximum degree of any vertex and simultaneously minimizing the maximum number of edges of any color. Our construction is based on finding a Hamiltonian path in the graph G (see [9]). Such a path contains exactly the required number $|Y_0 \cup Y_1| - 1 = 2^k - 1$ of edges $\{10y_0, 11y_1\}$, each corresponding to a basis vector $\{y_0 \oplus y_1, y_0, y_1\}$.

Suppose we have found a set B of $2^k - 1$ vectors corresponding to the edges in a Hamiltonian path. Since a path is acyclic, any non-empty subset of vectors in B induces a subgraph with at least one vertex of degree 1. Such a vertex is a position which is in the support of the subset vector sum, and furthermore, will remain so under the addition of any vectors in B'_k, which have no support in $Y_0 \cup Y_1$. This proves that if B_k is a basis of C_k, then B_{k+1} is a basis of C_{k+1}, as desired.

Table 1

Position	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Color	1	2	1	2	3	0	2	0	0	0	0	0	0	0	0
Degree	0	1	1	2	1	1	2	2	2	1	2	2	2	2	1
Total	1	3	2	4	4	1	4	2	2	1	2	2	2	2	1

For $k = 1, 2, 3$, we use the following Hamiltonian paths:

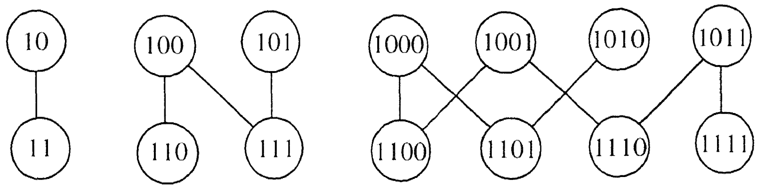


Table 1 gives the number of ones in each position of B_4, as the total number of basis vectors in which it appears as either a color $y_0 \oplus y_1$ or as a vertex y_i (its degree in the Hamiltonian path).

Since the maximum degree in a Hamiltonian path is 2, the width in positions $1\{0,1\}^{k-1}$ of any B_k will be at most 2. For $k \leqslant 4$, the table shows that the width in positions $0\{0,1\}^{k-1} \setminus \{0^k\}$ of B_k is at most 4. In order to continue our induction beyond $k = 4$, it suffices to find a Hamiltonian path in which each color $x \in X$ appears at most twice. Equivalently, we need to find a Hamiltonian *cycle* in which each $x \in X$ colors *exactly* two edges. The reason we make the first 3 induction steps explicit is that such a Hamiltonian cycle does not exist in the complete bipartite graph on $\{1000, 1001, 1010, 1011\} \cup \{1100, 1101, 1110, 1111\}$. Instead we compensated for the triple use of the color 0101 in the third path by limiting the degree of node 5 to 1 in the second path.

3.1. *Hamiltonian cycles*

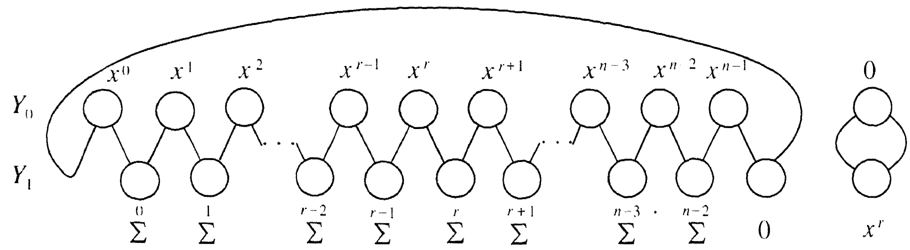
We turn to algebra to find the paths with the required color restrictions.

Let $GF(2)[x]$ denote the class of binary polynomials, that is, with coefficients 0 or 1, and addition and multiplication mod 2. We borrow a result from finite field theory which says that for any k, there exists a *primitive* binary polynomial $f(x)$ of degree k. This means that $GF(2)[x]/(f)$, the class of residues modulo f, is a finite field whose multiplicative group is generated by x. In other words, the set $\{x^0, x^1, \ldots, x^{2^k-2}\}$ contains all $n = 2^k - 1$ non-zero elements.

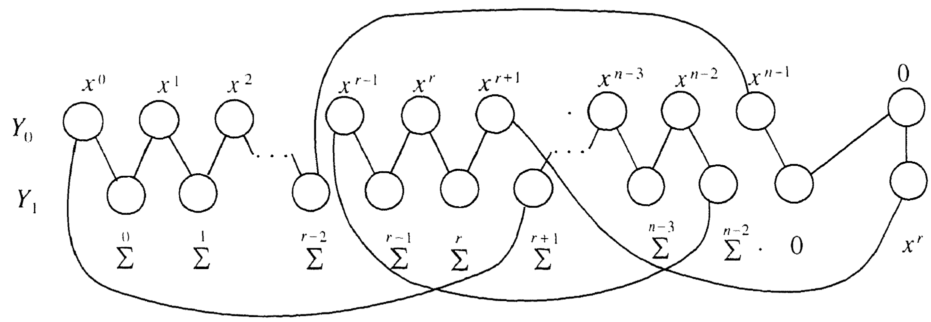
We can bring $GF(2)[x]/(f)$ in one–one correspondence to each of the three position sets X, Y_0 and Y_1 in the inductive step from $k+1$ to $k+2$, where they each have size 2^k. A position $p = p_1 \ldots p_{k+2}$ will correspond to the binary polynomial $\sum_{i=0}^{k-1} p_{k+2-i} x^i$, i.e. we ignore the two first bits that distinguish between X, Y_0, and Y_1. For example, with $k = 4$, $101101 \in Y_0$ corresponds to $x^3 + x^2 + 1$.

Let $(x+1)^{-1}$, the inverse of $x+1$, be equal to x^r for some r, $0 \leqslant r < 2^k - 1$. Note that $x^i \mapsto \sum_{j<i} x^j = (x^i+1)(x+1)^{-1} = x^r(x^i+1)$ is a bijection from all the non-zero elements of $GF(2)[x]/(f)$ to all elements except $x^r(0+1) = x^r$. Also, $\sum_{j<n} x^j = x^r(x^n+1) = x^r(1+1) = 0$.

These facts are the basis of the following cycle decomposition (using $\sum^i$ as a shorthand for $\sum_{j=0}^i x^j$):



The left cycle uses every color $\sum^i$, $0 \leqslant i < n$ exactly twice, once on the edge between $\sum^{i-1}$ and x^i, and once on the edge between x^{i+1} and $\sum^{i+1}$. The right cycle uses the single color not expressible as $\sum^i$, namely x^r, exactly twice. A series of 5 edge swaps transform the two cycles into the following Hamiltonian cycle:



We will refer to the 2-cycle decomposition as 2-cycle and to the Hamiltonian cycle as 1-cycle. The edge between $x^0 = 1$ and 0 in the 2-cycle has color 1, as does the edge between x^{r+1} and x^r in the 1-cycle, since $x^{r+1} + x^r = x^r(x+1) = 1$. The edge between $\sum^{r-2}$ and x^{r-1} in the 2-cycle has color $\sum^{r-1}$, as does the edge between $x^0 = 1$ and $\sum^{r+1}$ in the 1-cycle, since $\sum^{r+1} + 1 = \sum^{r-1} + x^{r+1} + x^r + 1 = \sum^{r-1}$. The edge between x^{r+1} and $\sum^{r+1}$ in the 2-cycle has color $\sum^r$, as does the edge between $\sum^{r-2}$ and x^{n-1} in the 1-cycle, since $\sum^{r-2} + x^{n-1} = \sum^r + x^r + x^{r-1} + x^{-1} = \sum^r + x^{-1}(x^{r+1} + x^r + 1) = \sum^r$. The edge between $\sum^{n-2}$ and x^{n-1} in the 2-cycle has color $\sum^{n-1} = 0$, as does the edge between 0 and 0 in the 1-cycle. The edge between 0 and x^r in the 2-cycle has color x^r, as does the edge between x^{r-1} and $\sum^{n-2}$ in the 1-cycle, since $x^{r-1} + \sum^{n-2} = x^{r-1} + x^{-1} = x^r + x^{-1}(x^{r+1} + x^r + 1) = x^r$.

It remains to show that this transformation does not suffer from r being too close to 0 or $n-1$. Indeed, $x^{r+1} + x^r + 1 = 0$ implies that $r + 1 \geqslant k \geqslant 3$, hence $r - 1 > 1$

and we are safe on the left. Similarly, $x^{n-r}+x+1=(x^r)^{-1}+x+1=0$ implies that $n-r\geqslant k\geqslant 3$, hence $r+1\leqslant n-2$, so we are safe on the right too.

Altogether, this shows

Theorem 1. *For any k, C_k has a* $(3,4)$*-basis.*

An n-dimensional hypercube of cliques is the cross product of an $(n-\lfloor\log r\rfloor)$-dimensional hypercube and a complete graph with $2^{\lfloor\log r\rfloor}$ nodes. By Theorem 1, we have

Corollary 2. *There is a one-to-one embedding of a hypercube of cliques in a same-sized hypercube with dilation* 3 *and congestion* 10.

Proof. See [6]. $\square$

4. On (3, 3) bases

In this section we give a sufficient condition for the existence of a $(3,3)$-basis for C_k. Suppose some degree k primitive polynomial $h(x)$ is the gcd of a trinomial $f(x)=1+x^j+x^m$ and x^n+1. Then C_k has a $(3,3)$-basis, constructed as follows. Consider the $n\times n$ circulant matrix F generated by f; the ith column F_i of this matrix $(i=0,\dots,n-1)$, is formed by the coefficients of $x^i f(x) \bmod x^n+1$. For example, with $n=7$, $h(x)=f(x)=1+x+x^3$ generates the matrix

$$F=\begin{pmatrix}1&0&0&0&1&0&1\\1&1&0&0&0&1&0\\0&1&1&0&0&0&1\\1&0&1&1&0&0&0\\0&1&0&1&1&0&0\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{pmatrix}.$$

We use the fact that $h(x)$ is primitive to define a column reordering of A_k, called A'_k, whose ith column corresponds to $x^i \bmod h(x)$. Now A'_kF_i corresponds to $x^i f(x) \bmod x^n+1 \bmod h(x)=x^i f(x) \bmod h(x)=0$, since $h(x)$ divides both $f(x)$ and x^n+1. Thus, all columns of F are in the nullspace C'_k of A'_k.

From a theorem of König and Rados [7], it follows that the rank of F is $n-\deg(\gcd(f(x),x^n+1))=n-\deg(h(x))=n-k$. Now if some column i is linearly dependent on columns $0,\dots,i-1$, then, since F is circulant, column $i+1$ is linearly dependent on columns $1,\dots,i$ and therefore also on columns $0,\dots,i-1$. Similarly, columns $i+2,\dots,n-1$ would be linearly dependent on the first i columns. Thus, the

Table 2
Trinomials $f(x) = x^m + x^j + 1$ that imply the existence of (3,3)-bases

k	m	j	k	m	j	k	m	j
8	13	1	67	76	29	120	174	31
12	19	6	69	75	23	122	128	15
13	16	3	70	82	15	125	128	3
14	17	2	72	93	7	126	141	70
16	29	6	74	80	39	128	131	50
19	22	3	75	77	4	131	138	61
24	55	6	76	88	43	133	136	43
26	29	12	77	80	9	136	139	30
27	29	1	78	89	2	138	183	23
30	41	12	80	83	23	139	142	3
32	59	29	82	85	19	141	148	71
34	37	6	83	85	14	143	147	1
37	43	4	85	93	28	144	159	14
38	42	1	86	91	22	146	149	6
40	43	3	88	154	37	147	149	19
42	51	7	90	111	28	149	151	2
43	53	2	91	99	13	152	155	38
44	52	15	92	103	39	154	157	22
45	59	12	96	123	1	155	158	75
46	58	9	99	101	13	156	188	59
48	70	27	101	103	2	157	164	25
50	54	7	102	115	3	158	167	54
51	53	4	104	109	9	160	177	19
53	61	28	107	109	8	162	166	27
54	93	23	109	118	21	163	171	70
56	67	31	110	117	19	164	189	68
59	61	26	112	133	1	165	173	42
61	66	17	114	118	7	166	186	53
62	77	30	115	125	6	168	179	38
64	74	21	116	136	1	171	173	10
66	83	20	117	123	31			

first $n - k$ columns of F must actually be linearly independent, else the rank of F would be less than $n - k$. This shows that $F_0, \dots, F_{n-k-1}$ forms a basis of C'_k, and, by an appropriate permutation of dimensions, a basis of C_k.

The existence of degree k primitive polynomials $h(x)$ that are the gcd of a trinomial $f(x) = 1 + x^m + x^j$ and $x^n + 1$, is demonstrated in Table 2 for $k \leqslant 171$. Only those k for which there is no primitive trinomial of degree k are listed; see Stahnke [11] for a table of primitive binary polynomials up to degree 171. Therefore, we pose the following:

Conjecture 1. *There always exists a trinomial $f(x)$ such that* $\gcd(f(x), x^{2^k-1} + 1)$ *is a primitive polynomial of degree k over GF(2), for any k. Consequently, any C_k has a (3,3)-basis.*

The subsequent effort by [4] shows the conjecture to hold through all $k \leqslant 500$.

Acknowledgements

The authors would like to thank Dan Pritikin and Gary Mullen for the careful reading of the manuscript and helpful suggestions.

References

[1] W. Aiello and T. Leighton, Coding theory, hypercube embeddings, and fault tolerance, in: *Proc. 3rd Ann. ACM Symp. on Parallel Algorithms and Architectures* (1991) 125–136; *IEEE Trans. Computer*, to appear.

[2] E. Assmus, Jr and H. Mattson, On tactical configurations and error-correcting-codes, *J. Combin. Theory* **2** (1967) 243–257.

[3] L. Babai, H. Oral and K. Phelps, Eulerian self-dual codes, *SIAM J. Discrete Math.* **7** (1994) 325–330.

[4] I.F. Blake, S. Gao and R.J. Lambert, Construction and distribution problem for irreducible trinomials over finite fields, in: *Proc. Holloway Conf. on Finite Fields* (Oxford Univ. Press, Oxford, 1995), to appear.

[5] R.H. Hamming, Error detecting and error correcting codes, *Bell System Tech. Journal* **29** (1950) 147–160.

[6] T. Leighton, *Introduction to Parallel Algorithms and Architectures: Arrays · Trees · Hypercubes*, Ch. 3 (Morgan Kaufmann, San Mateo, CA, 1992) 430.

[7] R. Lidl and H. Niederreiter, *Finite Fields* (Addison-Wesley, CA, 1983).

[8] V. Pless, *Introduction to the Theory of Error-Correcting-Codes* (Wiley, New York, 1989).

[9] D. Pritikin, Graph embeddings from Hamming bases, *DIMACS Workshops on Interconnection Networks and Mapping and Scheduling Parallel Computations*, February 1994.

[10] A. Reddy, Parallel input/output architectures for multiprocessors, Ph.D. Dissertation. Dept. of Electronical and Computer Engineering, Univ. of Illinois, Urbana, 1990.

[11] W. Stahnke, Primitive binary polynomials, *Math. Comput.* **124** (1973) 977–980.

[12] L. Zhang, A new bound for the width of Hamming codes, in: *Proc. 6th Internat. Conf. on Computing and Information*, 1994, to appear.