Fault-Tolerant Graphs for Tori

Toshinori Yamada, Shuichi Ueno

Department of Electrical and Electronic Engineering, Tokyo Institute of Technology, Tokyo 152, Japan

Received 3 September 1996; accepted 30 April 1998

Abstract: Motivated by the design of fault-tolerant multiprocessor interconnection networks, this paper considers the following problem: Given a positive integer t and a graph H, construct a graph G from H by adding a minimum number $\Delta(t, H)$ of edges such that even after deleting any t edges from G the remaining graph contains H as a subgraph. We estimate $\Delta(t, H)$ for the torus, which is well known as a very important interconnection network for multiprocessor systems. © 1998 John Wiley & Sons, Inc. Networks 32: 181–188, 1998

1. INTRODUCTION

Motivated by the design of fault-tolerant multiprocessor interconnection networks, this paper considers the following problem: Given a positive integer t and a graph H, construct a graph G from H by adding a minimum number of edges such that even after deleting any t edges from G the remaining graph contains H as a subgraph. We construct such graphs by adding a small number of edges for the torus, which is well known as an important interconnection network for multiprocessor systems. Many related results can be found in the literature.

Let G be a graph and let $V(G)$ and $E(G)$ denote the vertex set and the edge set of G, respectively. For any $S \subseteq E(G)$, $G \backslash S$ is the graph obtained from G by deleting the edges of S.

Let t be a positive integer and let H be a graph. A graph G is called a t-EFT (t-edge-fault-tolerant) graph for H if $G \backslash S$ contains H as a subgraph for every $S \subseteq E(G)$, with $|S| \leq t$. Let $\Delta(t, H)$ denote the minimum number of edges added to H to construct a t-EFT graph for H with $|V(H)|$ vertices.

Correspondence to: S. Ueno; e-mail: ueno@ss.titech.ac.jp

Let $D_n(k)$ denote the n-dimensional $k \times k \times \cdots \times k$ torus. $D_n(2)$ is known as the n-cube. The following results can be found in the literature:

(**I**) [18, 21, 26] $\Delta(1, D_n(2)) = 2^{n-1}$.

(**II**) [28] $\Delta(t, D_n(2)) = O\left(t2^{n-1}\log_2\left(\frac{n}{t-1} + c\right)\right)$,

if $t \geq 2$, where $c = 1 + \log_2 e$.

(**III**) [10] $\Delta(t, D_n(p)) \leq tp^n$, if $t \leq p + 1 - n$ and p is a prime.

In this paper, we generalize the results above and show the following:

1. $\Delta(1, D_n(k)) \leq k^n$, if $k \geq 3$.
2. $\Delta(t, D_n(p^l)) \leq (t-1)p^{ln}\{2\log_p(n/(t-1) + c_p) + c_p\} + p^{ln}$, if $t \geq 2$ and $p^l \geq 3$,
3. $\Delta(t, D_n(p^l)) \leq tp^{ln}$, if $t \leq p + 1 - n$ and $p^l \geq 3$,

where p is a prime, k and l are positive integers, and $c_p = 1 + \log_p e$.

The notion of the matric graph was introduced in [28] as a natural generalization of the hypercube. The upper

CCC 0028-3045/98/030181-08

bound for $\Delta(t, D_n(2))$ in (II) was proved by constructing matric graphs associated with basis matrices of error-correcting binary linear codes. The essentially same construction was proposed in [13] independent of [28]. Here, we further extend the notion of the matric graph to be a generalization of the torus. The upper bounds for $\Delta(t, D_n(k))$ in (1), (2), and (3) are proved by constructing t-EFT matric graphs for $D_n(k)$ associated with basis matrices of error-correcting linear codes. It is interesting that the t-EFT matric graphs for $D_n(k)$ proposed here have a strong fault-tolerance property. We show that even after deleting tk^n edges of t different dimensions from a t-EFT matric graph for $D_n(k)$ the remaining graph still contains $D_n(k)$ as a subgraph.

2. MATRIC GRAPHS AND TORI

Let $k \geq 2$ be an integer and let $[k] = \{0, 1, \ldots, k-1\}$. The n-dimensional $k \times k \times \cdots \times k$ torus, denoted by $D_n(k)$, is defined as follows: $V(D_n(k)) = [k]^n$; $E(D_n(k)) = \{(\boldsymbol{u}, \boldsymbol{v}) | \exists i\ v_i = (u_i \pm 1) \bmod k, \forall j \neq i\ u_j = v_j\}$, where $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ and $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$. $D_n(2)$ is called the n-cube (n-dimensional cube). It is easy to see that $D_n(k)$ is connected and $|V(D_n(k))| = k^n$. If $k \geq 3$, $|E(D_n(k))| = nk^n$, since the degree of each vertex of $D_n(k)$ is $2n$. Since the degree of each vertex of $D_n(2)$ is n, $|E(D_n(2))| = 2^{n-1}$. An edge $(\boldsymbol{u}, \boldsymbol{v})$ is called an i-edge (i-dimensional edge) if $v_i = (u_i \pm 1) \bmod k$ and $u_j = v_j$ for any $j \neq i$.

Let M be an $m \times n$ matrix over $[k]$, which is an m by n matrix consisting of 0's, 1's, ..., and $(k-1)$'s. Let $\boldsymbol{r}_i$ and $\boldsymbol{c}_j$ denote the i-th row and the j-th column of M, respectively. Define $R(M) = \{\boldsymbol{r}_1, \boldsymbol{r}_2, \ldots, \boldsymbol{r}_m\}$ and $C(M) = \{\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n\}$.

The matric graph associated with an $m \times n$ matrix M over $[k]$, denoted by $G_k(M)$, is defined as follows: $V(G_k(M)) = [k]^n$; any two vertices $\boldsymbol{u}$ and $\boldsymbol{v}$ are joined by $|\{\boldsymbol{r} \in R(M) | \boldsymbol{u} + \boldsymbol{v} = \boldsymbol{r}\}|$ parallel edges if $k = 2$, and $|\{\boldsymbol{r} \in R(M) | \boldsymbol{u} = \boldsymbol{v} + \boldsymbol{r}\}| + |\{\boldsymbol{r} \in R(M) | \boldsymbol{v} = \boldsymbol{u} + \boldsymbol{r}\}|$ parallel edges otherwise, where vector addition is performed modulo k. An edge $(\boldsymbol{u}, \boldsymbol{v})$ of $G_k(M)$ is said to be of dimension $\boldsymbol{r} (\in R(M))$ if $\boldsymbol{u} = \boldsymbol{v} + \boldsymbol{r}$ or $\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{r}$. For $\boldsymbol{r} \in R(M)$, $E_k(\boldsymbol{r})$ is the set of all edges of dimension $\boldsymbol{r}$ of $G_k(M)$. For $S \subseteq R(M)$, $E_k(S) = \cup_{\boldsymbol{r} \in S} E_k(\boldsymbol{r})$. If $k \geq 3$, each vertex of $G_k(M)$ is incident to two edges of dimension $\boldsymbol{r}$ for any $\boldsymbol{r} \in R(M)$, and so the degree of each vertex of $G_k(M)$ is $2m$. Thus, $|E(G_k(M))| = mk^n$ if $k \geq 3$. Since each vertex of $G_2(M)$ is incident to an edge of dimension $\boldsymbol{r}$ for any $\boldsymbol{r} \in R(M)$, the degree of each vertex of $G_2(M)$ is m. Thus, $|E(G_2(M))| = m2^{n-1}$. For $S \subseteq R(M)$, let $M \backslash S$ denote the matrix obtained from a matrix M by deleting the rows of S. It is easy to see the following two lemmas from the definition of the matric graph:

Lemma 1. *If I_n is the $n \times n$ unit matrix over $[k]$, then $G_k(I_n)$ is isomorphic to $D_n(k)$. Moreover, the edges of dimension $\boldsymbol{r}_i$ of $G_k(I_n)$ correspond to the i-edges of $D_n(k)$.*

Lemma 2. *$G_k(M \backslash S)$ is isomorphic to $G_k(M) \backslash E_k(S)$.*

Lemma 3. *If a matrix M over $[k]$ has a column consisting of 0's, then $G_k(M)$ is disconnected.*

Proof. Assume that $\boldsymbol{c}_i = \boldsymbol{0}$ for some i. Define $V_j = \{\boldsymbol{v} \in V(G_p(M)) | v_i = j\}$ for any $j \in [k]$, where $\boldsymbol{v} = (v_1, \ldots, v_n)$. $(V_0, \ldots, V_{k-1})$ is a partition of $V(G_k(M))$. Since $\boldsymbol{c}_i = \boldsymbol{0}$, there exists no edge joining a vertex in V_0 and a vertex in $V(G_k(M)) - V_0 = V_1 \cup \cdots \cup V_{k-1}$. Hence, $G_k(M)$ is disconnected. ■

Let p be a prime. It should be noted that the addition and multiplication modulo p corresponds to the addition and multiplication over $GF(p)$, respectively.

Lemma 4. *If M' is a matrix obtained from an $m \times n$ matrix M over $GF(p)$ by elementary column operations, then $G_p(M')$ is isomorphic to $G_p(M)$.*

Proof. Let $\lambda \neq 0$, $\lambda \in [p]$. It suffices to prove the following: (i) If M' is a matrix obtained from M by multiplying column $\boldsymbol{c}_{j_1}$ by λ, $1 \leq j_1 \leq n$, then $G_p(M')$ is isomorphic to $G_p(M)$; (ii) if M' is a matrix obtained from M by exchanging column $\boldsymbol{c}_{j_1}$ with column $\boldsymbol{c}_{j_2}$, $1 \leq j_1 < j_2 \leq n$, then $G_p(M')$ is isomorphic to $G_p(M)$; and (iii) if M' is a matrix obtained from M by adding column $\lambda \boldsymbol{c}_{j_2}$ to $\boldsymbol{c}_{j_1}$, $j_1 \neq j_2$, then $G_p(M')$ is isomorphic to $G_p(M)$.

Proof of (i). Let φ_1 be a mapping from $V(G_p(M))$ to $V(G_p(M'))$ such that

$$\varphi_1(\boldsymbol{v}) = (v_1, \ldots, \lambda v_{j_1}, \ldots, v_n).$$

If $\varphi_1(\boldsymbol{u}) = \varphi_1(\boldsymbol{v})$, then $u_j = v_j$ $(j \neq j_1)$ and $\lambda u_{j_1} = \lambda v_{j_1}$. Thus, $u_{j_1} = v_{j_1}$, and so $\boldsymbol{u} = \boldsymbol{v}$. Thus, φ_1 is a one-to-one mapping. Since $|V(G_p(M))| = |V(G_p(M'))| = p^n$, φ_1 is a bijection.

Let $\boldsymbol{r}_i'$ denote the i-th row of M'. If $\boldsymbol{r}_i = (x_1, \ldots, x_n)$, then $\boldsymbol{r}_i' = (x_1, \ldots, \lambda x_{j_1}, \ldots, x_n)$. Since $\boldsymbol{u} + \boldsymbol{r}_i = \boldsymbol{v}$ if and only if $\varphi_1(\boldsymbol{u}) + \boldsymbol{r}_i' = \varphi_1(\boldsymbol{v})$, and $\boldsymbol{v} + \boldsymbol{r}_i = \boldsymbol{u}$ if and only if $\varphi_1(\boldsymbol{v}) + \boldsymbol{r}_i' = \varphi_1(\boldsymbol{u})$, we conclude that $(\boldsymbol{u}, \boldsymbol{v}) \in E(G_p(M))$ if and only if $(\varphi_1(\boldsymbol{u}), \varphi_1(\boldsymbol{v})) \in E(G_p(M'))$. Thus, $G_p(M)$ is isomorphic to $G_p(M')$.

Proof of (ii). Let φ_2 be a mapping from $V(G_p(M))$ to $V(G_p(M'))$ such that

$$\varphi_2(\boldsymbol{v}) = (v_1, \ldots, v_{j_2}, \ldots, v_{j_1}, \ldots, v_n).$$

If $\varphi_2(\boldsymbol{u}) = \varphi_2(\boldsymbol{v})$, then $u_j = v_j$ $(1 \le j \le n)$, and so $\boldsymbol{u} = \boldsymbol{v}$. Thus, φ_2 is a bijection.

If $\boldsymbol{r}_i = (x_1, \ldots, x_n)$, then $\boldsymbol{r}_i' = (x_1, \ldots, x_{j_2}, \ldots, x_{j_1}, \ldots, x_n)$. Since $\boldsymbol{u} + \boldsymbol{r}_i = \boldsymbol{v}$ if and only if $\varphi_2(\boldsymbol{u}) + \boldsymbol{r}_i' = \varphi_2(\boldsymbol{v})$, and $\boldsymbol{v} + \boldsymbol{r}_i = \boldsymbol{u}$ if and only if $\varphi_2(\boldsymbol{v}) + \boldsymbol{r}_i' = \varphi_2(\boldsymbol{u})$, we conclude that $(\boldsymbol{u}, \boldsymbol{v}) \in E(G_p(M))$ if and only if $(\varphi_2(\boldsymbol{u}), \varphi_2(\boldsymbol{v})) \in E(G_p(M'))$. Thus, $G_p(M)$ is isomorphic to $G_p(M')$.

Proof of (iii). Let φ_3 be a mapping from $V(G_p(M))$ to $V(G_p(M'))$ such that

$$\varphi_3(\boldsymbol{v}) = (v_1, \ldots, v_{j_1} + \lambda v_{j_2}, \ldots, v_n).$$

If $\varphi_3(\boldsymbol{u}) = \varphi_3(\boldsymbol{v})$, then $u_j = v_j$ $(j \ne j_1)$ and $u_{j_1} + \lambda u_{j_2} = v_{j_1} + \lambda v_{j_2}$. Since $u_{j_2} = v_{j_2}$, we obtain $u_{j_1} = v_{j_1}$, and so $\boldsymbol{u} = \boldsymbol{v}$. Thus, φ_3 is a bijection.

If $\boldsymbol{r}_i = (x_1, \ldots, x_n)$, then $\boldsymbol{r}_i' = (x_1, \ldots, x_{j_1} + \lambda x_{j_2}, \ldots, x_n)$. Since $\boldsymbol{u} + \boldsymbol{r}_i = \boldsymbol{v}$ if and only if $\varphi_3(\boldsymbol{u}) + \boldsymbol{r}_i' = \varphi_3(\boldsymbol{v})$, and $\boldsymbol{v} + \boldsymbol{r}_i = \boldsymbol{u}$ if and only if $\varphi_3(\boldsymbol{v}) + \boldsymbol{r}_i' = \varphi_3(\boldsymbol{u})$, we conclude that $(\boldsymbol{u}, \boldsymbol{v}) \in E(G_p(M))$ if and only if $(\varphi_3(\boldsymbol{u}), \varphi_3(\boldsymbol{v})) \in E(G_p(M'))$. Thus, $G_p(M)$ is isomorphic to $G_p(M')$. ■

Theorem 1. *For any $n \times n$ matrix M over $GF(p)$, $G_p(M)$ is isomorphic to $D_n(p)$ if and only if M is nonsingular.*

Proof. If M is nonsingular, then we can obtain the unit matrix I_n from M by elementary column operations. Thus, $G_p(M)$ is isomorphic to $D_n(p)$ by Lemmas 1 and 4.

If M is singular, then we can obtain a matrix with a column consisting of 0's from M by elementary column operations. Thus, $G_p(M)$ is not isomorphic to $D_n(p)$, since $G_p(M)$ is disconnected by Lemmas 3 and 4. ■

Corollary 1. *For any $m \times n$ matrix M over $GF(p)$, $G_p(M)$ contains $D_n(p)$ as a subgraph if and only if the rank of M is n.*

Proof. If the rank of M is n, then there exists $S \subset R(M)$ with $|S| = m - n$ such that $M \backslash S$ is an $n \times n$ nonsingular matrix over $GF(p)$. Thus, $G_p(M \backslash S)$ is isomorphic to $D_n(p)$ by Theorem 1, and so $G_p(M)$ contains $D_n(p)$ as a subgraph by Lemma 2.

If the rank of M is less than n, then we can obtain a matrix with a column consisting of 0's from M by elementary column operations. Thus, $G_p(M)$ is disconnected by Lemmas 3 and 4. Since $|V(G_p(M))| = |V(D_n(p))| = p^n$, we conclude that $G_p(M)$ does not contain $D_n(p)$ as a subgraph. ■

For any vector $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ consisting of integers, $\boldsymbol{v} \bmod k$ is defined as $(v_1 \bmod k, v_2 \bmod k, \ldots, v_n \bmod k)$. An $m \times n$ matrix M over $[k]$ is said to have property $\mathcal{J}_k$ if the following condition is satisfied: If $(a_1\boldsymbol{r}_1 + a_2\boldsymbol{r}_2 + \cdots + a_m\boldsymbol{r}_m) \bmod k = \boldsymbol{0}$ holds for $a_1, a_2, \ldots, a_m \in [k]$, then $a_1 = a_2 = \cdots = a_m = 0$. It should be noted that $\mathcal{J}_k$ is a generalization of the linear independency. The following theorem does hold even if k is not a prime:

Theorem 2. *For any $n \times n$ matrix M over $[k]$, $G_k(M)$ is isomorphic to $D_n(k)$ if and only if M has property $\mathcal{J}_k$.*

Proof. In what follows, we denote $G_k(M)$ and $D_n(k)$ by G and D, respectively.

Assume that M has property $\mathcal{J}_k$. Let ϕ be a mapping from $V(D)$ to $V(G)$ such that $\phi(\boldsymbol{v}) = (v_1\boldsymbol{r}_1 + v_2\boldsymbol{r}_2 + \cdots + v_n\boldsymbol{r}_n) \bmod k$, where $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$. If $\phi(\boldsymbol{u}) = \phi(\boldsymbol{v})$, then

$$\phi(\boldsymbol{u}) - \phi(\boldsymbol{v}) = (u_1\boldsymbol{r}_1 + u_2\boldsymbol{r}_2 + \cdots + u_n\boldsymbol{r}_n) \bmod k - (v_1\boldsymbol{r}_1 + v_2\boldsymbol{r}_2 + \cdots + v_n\boldsymbol{r}_n) \bmod k = \boldsymbol{0},$$

that is,

$$((u_1 - v_1)\boldsymbol{r}_1 + (u_2 - v_2)\boldsymbol{r}_2 + \cdots + (u_n - v_n)\boldsymbol{r}_n) \bmod k = \boldsymbol{0}. \quad (1)$$

For any $i = 1, 2, \ldots, n$, let $a_i = u_i - v_i$ if $u_i \ge v_i$, and $a_i = u_i - v_i + k$ otherwise. It should be noted that $a_i \in [k]$, and if $a_i = 0$, then $u_i = v_i$. By Eq. (1), we have

$$(a_1\boldsymbol{r}_1 + a_2\boldsymbol{r}_2 + \cdots + a_n\boldsymbol{r}_n) \bmod k = \boldsymbol{0},$$

and so $a_i = 0$ for any i since M has property $\mathcal{J}_k$. Thus, $u_i = v_i$ for any $i = 1, 2, \ldots, n$, and ϕ is a one-to-one mapping. Since $|V(D)| = |V(G)| = k^n$, ϕ is a bijection.

Now we prove that ϕ is an isomorphism between G and D. It is sufficient to show that $(\boldsymbol{u}, \boldsymbol{v}) \in E(D)$ if and only if $(\phi(\boldsymbol{u}), \phi(\boldsymbol{v})) \in E(G)$. If $(\boldsymbol{u}, \boldsymbol{v}) \in E(D)$, then $\boldsymbol{v} = (\boldsymbol{u} + \boldsymbol{e}_i) \bmod k$ or $\boldsymbol{u} = (\boldsymbol{v} + \boldsymbol{e}_i) \bmod k$ for some i, where $\boldsymbol{e}_i$ is the i-dimensional unit vector. Thus, $\phi(\boldsymbol{v}) = (\phi(\boldsymbol{u}) + \boldsymbol{r}_i) \bmod k$ or $\phi(\boldsymbol{u}) = (\phi(\boldsymbol{v}) + \boldsymbol{r}_i) \bmod k$, and so $(\phi(\boldsymbol{u}), \phi(\boldsymbol{v})) \in E(G)$. If $(\phi(\boldsymbol{u}), \phi(\boldsymbol{v})) \in E(G)$, then $\phi(\boldsymbol{v}) = (\phi(\boldsymbol{u}) + \boldsymbol{r}_i) \bmod k$ or $\phi(\boldsymbol{u}) = (\phi(\boldsymbol{v}) + \boldsymbol{r}_i) \bmod k$ for some i. Thus, $\phi(\boldsymbol{v}) = (\phi(\boldsymbol{u}) + \phi(\boldsymbol{e}_i)) \bmod k$ or $\phi(\boldsymbol{u}) = (\phi(\boldsymbol{v}) + \phi(\boldsymbol{e}_i)) \bmod k$, that is, $\phi(\boldsymbol{v}) = \phi((\boldsymbol{u} + \boldsymbol{e}_i) \bmod k)$ or $\phi(\boldsymbol{u}) = \phi((\boldsymbol{v} + \boldsymbol{e}_i) \bmod k)$. Since ϕ is a bijection from $[k]^n$ to $[k]^n$, $\boldsymbol{v} = (\boldsymbol{u} + \boldsymbol{e}_i) \bmod k$ or $\boldsymbol{u} = (\boldsymbol{v} + \boldsymbol{e}_i) \bmod k$, and so $(\boldsymbol{u}, \boldsymbol{v}) \in E(D)$. Thus, $(\boldsymbol{u}, \boldsymbol{v}) \in E(D)$ if and only if $(\phi(\boldsymbol{u}), \phi(\boldsymbol{v})) \in E(G)$. Hence, ϕ is an isomorphism and G is isomorphic to D.

Assume that M does not have property $\mathcal{J}_k$. Since ϕ is not a one-to-one mapping and $|V(D)| = |V(G)| = k^n$, there exists some $\boldsymbol{v} \notin \phi(V(D))$. If G is connected, then there exists a path P from $\boldsymbol{0}$ to $\boldsymbol{v}$. Let $P = \boldsymbol{v}_0\boldsymbol{v}_1 \cdots \boldsymbol{v}_d$, where $\boldsymbol{v}_0 = \boldsymbol{0}$ and $\boldsymbol{v}_d = \boldsymbol{v}$. Then, for any $j = 1, 2, \ldots, d$, there exists some i such that $\boldsymbol{v}_j = (\boldsymbol{v}_{j-1} + \boldsymbol{r}_i) \bmod k$ or $\boldsymbol{v}_j = (\boldsymbol{v}_{j-1} - \boldsymbol{r}_i) \bmod k$. Since $\boldsymbol{v} = \sum_{j=1}^{d} (\boldsymbol{v}_j - \boldsymbol{v}_{j-1})$, $\boldsymbol{v}$ can

be expressed as $\boldsymbol{v} = (a_1\boldsymbol{r}_1 + a_2\boldsymbol{r}_2 + \cdots + a_n\boldsymbol{r}_n) \bmod k$ for some integers $a_1, a_2, \ldots,$ and a_n. Thus, we conclude that for $\mathbf{a} = (a_1, a_2, \ldots, a_n) \bmod k \in V(D)$, $\phi(\mathbf{a}) = \boldsymbol{v}$, a contradiction. Thus, G is disconnected, and, hence, G is not isomorphic to D. ■

3. t-DFT MATRIC GRAPHS FOR $D_n(k)$

Let M be an $m \times n$ matrix over $[k]$. $G_k(M)$ is called a t-DFT (t-dimension-fault-tolerant) matric graph for $D_n(k)$ if $G_k(M)\backslash E_k(S)$ $(=G_k(M\backslash S))$ contains $D_n(k)$ as a subgraph for any $S \subseteq R(M)$, with $|S| \leq t$. Define $\Lambda(t, n, k) = \min\{|E(G_k(M))| - |E(D_n(k))| \mid G_k(M)$: t-DFT matric graph for $D_n(k)\}$. Since the degree of each vertex of $G_k(M)$ is m if $k = 2$ and $2m$ otherwise, the problem of finding $\Lambda(t, n, k)$ is equivalent to the one of finding the minimum number of rows of a matrix M such that $G_k(M)$ is a t-DFT matric graph for $D_n(k)$.

3.1. The Case When k is a Prime p

The following theorem characterizes the t-DFT matric graph for $D_n(p)$. Recall that the Hamming weight of a vector $\boldsymbol{v}$ over $GF(p)$ is the number of nonzero elements of $\boldsymbol{v}$:

Theorem 3. *For any $m \times n$ matrix M over $GF(p)$, $G_p(M)$ is a t-DFT matric graph for $D_n(p)$ if and only if the Hamming weight of any linear combination of $C(M)$ is at least $t + 1$.*

Proof. Assume that there exists a linear combination of $C(M)$ such that its Hamming weight is at most t. Then, we can obtain a matrix M' with a column (say, the j-th column) of Hamming weight at most t from M by some elementary column operations. Let S be the set of rows of M corresponding to the rows S' of M' whose j-th elements are nonzeros. Since the j-th column of $M'\backslash S'$ consists of 0's, $G_p(M'\backslash S')$ does not contain $D_n(p)$ as a subgraph by Corollary 1. Since $G_p(M\backslash S)$ is isomorphic to $G_p(M'\backslash S')$ by Lemma 4 and $|S| = |S'| \leq t$, we conclude that $G_p(M)$ is not a t-DFT matric graph for $D_n(p)$.

Conversely, assume that the Hamming weight of any linear combination of $C(M)$ is at least $t + 1$. Then, $C(M\backslash S)$ is linearly independent for any $S \subseteq R(M)$ with $|S| \leq t$, and the rank of $M\backslash S$ is n. Thus, $G_p(M\backslash S)$ contains $D_n(p)$ as a subgraph by Corollary 1, and we conclude that $G_p(M)$ is a t-DFT matric graph for $D_n(p)$. ■

Theorem 3 means that for any $m \times n$ matrix M over $GF(p)$, $G_p(M)$ is a t-DFT matric graph for $D_n(p)$ if and only if $C(M)$ is a basis of an n-dimensional vector space over $GF(p)$ such that the Hamming weight of any nonzero vector is at least $t + 1$. Thus, t-DFT matric graphs can be characterized by error-correcting linear codes. Recall that the minimum distance for a linear code C is $\min\{d_H(\boldsymbol{u}, \boldsymbol{v}) \mid \boldsymbol{u} \neq \boldsymbol{v}, \boldsymbol{u}, \boldsymbol{v} \in C\}$, where $d_H(\boldsymbol{u}, \boldsymbol{v})$ is the Hamming distance between $\boldsymbol{u}$ and $\boldsymbol{v}$, that is, the number of positions in which they differ.

Theorem 4. *For any $m \times n$ matrix M over $GF(p)$, $G_p(M)$ is a t-DFT matric graph for $D_n(p)$ if and only if $C(M)$ is a basis of an n-dimensional linear code over $GF(p)$ with minimum distance at least $t + 1$.*

The following bounds for the existence of n-dimensional linear codes over $GF(p)$ with minimum distance at least $t + 1$ are well known. (See, e.g., [24]).

Theorem I. *If there exists an n-dimensional linear code over $GF(p)$ with minimum distance at least $t + 1$ and length m, then*

$$p^{m-n} \geq \sum_{i=0}^{\lfloor t/2 \rfloor} (p-1)^i \binom{m}{i}.$$

■

Theorem II. *If*

$$p^{m-n} > \sum_{i=0}^{t-1} (p-1)^i \binom{m-1}{i},$$

then there exists an n-dimensional linear code over $GF(p)$ with minimum distance at least $t + 1$ and length m. ■

The inequalities of Theorems I and II are well known as Hamming-bound and Varsharmov–Gilbert-bound, respectively. It should be noted that Theorem II is proved constructively. In what follows, we estimate $\Lambda(t, n, p)$ from Theorems 4, I, and II. We need a few lemmas:

Lemma 5. *For $1 \leq k \leq m$,*

$$\left\{\frac{(p-1)m}{k}\right\}^k \leq \sum_{i=0}^{k} (p-1)^i \binom{m}{i} \leq p^k \binom{m}{k}.$$

Proof. Let $S_p(m, k) = \Sigma_{i=0}^{k} (p-1)^i \binom{m}{i}$.
First, consider the first inequality. Trivially,

$$S_p(m, k) \geq (p-1)^k \binom{m}{k} \geq (p-1)^k \times \frac{m(m-1)\cdots(m-k+1)}{k!} \geq (p-1)^k \left(\frac{m}{k}\right)^k.$$

Now consider the second inequality. By induction on m and k,

1. Since $S_p(m, 1) = (p-1)m + 1 \le pm$ and $S_p(k, k) = p^k$, the claim is true if $k = 1$ or $m = k$.
2. Let $2 \le k < m$ and assume that the claim is true for $S_p(m, k')$, $S_p(m'k)$, and $S_p(m', k')$ with $m > m'$ and $k > k'$. Since

$$\binom{m}{i} = \binom{m-1}{i} + \binom{m-1}{i-1}$$

for any i, $1 \le i \le m-1$, $S_p(m, k) = S_p(m-1, k) + (p-1)\cdot S_p(m-1, k-1)$. Thus,

$$S_p(m,k) \le p^k\binom{m-1}{k} + (p-1)\cdot p^{k-1}\binom{m-1}{k-1}$$

$$\le p^k\cdot\left\{\binom{m-1}{k} + \binom{m-1}{k-1}\right\} = p^k\binom{m}{k}. \quad \blacksquare$$

Lemma 6 [16].

$$\binom{m}{k} \le \left(\frac{em}{k}\right)^k. \quad \blacksquare$$

Lemma 7. *Let $y \ge 1 + \log_p e$. If $x - \log_p x \le y$, then $x \le y + 2\log_p y$.*

Proof. Assume contrary that $x > y + 2\log_p y$ and let $g(z) = z - \log_p z$. Since $g(z)$ is an increasing function for $z > \log_p e$ and $x > y + 2\log_p y \ge 1 + \log_p e$, we have

$$g(x) - y > g(y + 2\log_p y) - y$$

$$= 2\log_p y - \log_p(y + 2\log_p y) = \log_p \frac{y^2}{y + 2\log_p y}.$$

Since $y^2 \ge y + 2\log_p y$ for any $y \ge 1 + \log_p e$, we obtain $x - \log_p x > y$, which is a contradiction. $\blacksquare$

Theorem 5. *Let M be an $m \times n$ matrix over $GF(p)$. If $G_p(M)$ is a t-DFT matric graph for $D_n(p)$ $(t \ge 2)$, then*

$$m \ge n + \left\lfloor \frac{t}{2} \right\rfloor \log_p \frac{(p-1)n}{\lfloor t/2 \rfloor}.$$

Proof. If $G_p(M)$ is a t-DFT matric graph for $D_n(p)$, then $C(M)$ is a basis of an n-dimensional linear code over $GF(p)$ with minimum distance at least $t+1$ by Theorem 4. Thus, by Theorem I and Lemma 5, we have

$$p^{m-n} \ge \sum_{i=0}^{k} (p-1)^i\binom{m}{i} \ge \left\{\frac{(p-1)m}{k}\right\}^k,$$

where $k = \left\lfloor \frac{t}{2} \right\rfloor$. Hence,

$$m - n \ge k\log_p \frac{(p-1)m}{k} \ge k\log_p \frac{(p-1)n}{k}. \quad \blacksquare$$

Theorem 6. *There exists an $m \times n$ matrix M over $GF(p)$ such that $G_p(M)$ is a t-DFT matric graph for $D_n(p)$ $(t \ge 2)$ and*

$$m \le n + (t-1)\left\{2\log_p\left(\frac{n}{t-1} + c_p\right) + c_p\right\} + 1,$$

where $c_p = 1 + \log_p e$.

Proof. By Theorems 4 and II, if

$$p^{m-n} > \sum_{i=0}^{t-1} (p-1)^i\binom{m-1}{i}, \qquad (2)$$

then there exists an $m \times n$ matrix M over $GF(p)$ such that $G_p(M)$ is a t-DFT matric graph for $D_n(p)$. Let m' be the minimum number of m satisfying (2). Then,

$$p^{m'-1-n} \le \sum_{i=0}^{t-1} (p-1)^i\binom{m'-2}{i} \le \sum_{i=0}^{t-1} (p-1)^i\binom{m'-1}{i}.$$

Thus, by Lemmas 5 and 6,

$$p^{m'-1-n} \le \left\{\frac{ep(m'-1)}{t-1}\right\}^{t-1},$$

that is,

$$m' - 1 - n \le (t-1)\left(\log_p \frac{m'-1}{t-1} + 1 + \log_p e\right),$$

that is,

$$\frac{m'-1}{t-1} - \log_p \frac{m'-1}{t-1} \le \frac{n}{t-1} + c_p.$$

Since $c_p = 1 + \log_p e$, by putting $x = (m' - 1)/(t - 1)$ and $y = n/(t - 1) + c_p$ in Lemma 7, we obtain

$$\frac{m' - 1}{t - 1} \leq \frac{n}{t - 1} + c_p + 2 \log\left(\frac{n}{t - 1} + c_p\right).$$

Hence,

$$m' \leq n + (t - 1)\left\{2 \log\left(\frac{n}{t - 1} + c_p\right) + c_p\right\} + 1. \quad \blacksquare$$

Since the numbers of edges of $G_p(M)$ and $D_n(p)$ are mp^n and np^n, respectively, we obtain from Theorems 5 and 6 the following upper and lower bounds for $\Lambda(t, n, p)$:

Theorem 7. *For any prime $p \geq 3$,*

$$\left\lfloor \frac{t}{2} \right\rfloor p^n \log_p \frac{(p - 1)n}{\lfloor t/2 \rfloor} \leq \Lambda(t, n, p) \leq (t - 1)p^n\left\{2 \log_p\left(\frac{n}{t - 1} + c_p\right) + c_p\right\} + p^n,$$

where $t \geq 2$ and $c_p = 1 + \log_p e$. $\blacksquare$

Since the numbers of edges of $G_2(M)$ and $D_n(2)$ are $m2^{n-1}$ and $n2^{n-1}$, respectively, we obtain from Theorems 5 and 6

$$\left\lfloor \frac{t}{2} \right\rfloor 2^{n-1} \log_2 \frac{n}{\lfloor t/2 \rfloor} \leq \Lambda(t, n, 2) \leq (t - 1)2^{n-1}\left\{2 \log_2\left(\frac{n}{t - 1} + c_2\right) + c_2\right\} + 2^{n-1},$$

which was proved in [28]. We can show the precise value of $\Lambda(1, n, p)$ as follows:

Theorem 8. *$\Lambda(1, n, p) = p^n$ for any prime $p \geq 3$.*

Proof. If M is the $n \times (n + 1)$ matrix over $GF(p)$ obtained from I_n by adding a row consisting of 1's, then M satisfies the condition of Theorem 3 for $t = 1$. Thus, $\Lambda(1, n, p) \leq p^n$.

If M is an $m \times n$ matrix over $GF(p)$ such that $G_p(M)$ is a 1-DFT matric graph for $D_n(p)$, then $m \geq n + 1$, and so $\Lambda(1, n, p) \geq p^n$. $\blacksquare$

3.2. The Case When $k \geq 3$ Is an Integer

For any matrix $M = (m_{ij})$ consisting of integers, let $M \bmod k = (m_{ij} \bmod k)$.

Lemma 8. *Let $k = k_1k_2$, where $k_i \geq 2$ for $i = 1, 2$. Then, an $n \times n$ matrix M over $[k]$ has property $\mathcal{J}_k$ if and only if $M \bmod k_1$ has property $\mathcal{J}_{k_1}$ and $M \bmod k_2$ has property $\mathcal{J}_{k_2}$.*

Proof. Assume that M does not have property $\mathcal{J}_k$, that is, there exists some $a_1, a_2, \ldots, a_n \in [k]$, not all zero, such that

$$(a_1\boldsymbol{r}_1 + a_2\boldsymbol{r}_2 + \cdots + a_n\boldsymbol{r}_n) \bmod k = \mathbf{0}. \qquad (3)$$

Let $a_i' = a_i \bmod k_1$ for $i = 1, 2, \ldots, n$. Then, $(a_1'\boldsymbol{r}_1 + a_2'\boldsymbol{r}_2 + \cdots + a_n'\boldsymbol{r}_n) \bmod k_1 = \mathbf{0}$ by Eq. (3). Thus, if $a_i' \neq 0$ for some i, then $M \bmod k_1$ does not have property $\mathcal{J}_{k_1}$. If $a_i' = 0$ for any $i = 1, 2, \ldots, n$, then $a_i'' = a_i/k_1 \in [k_2]$ for any $i = 1, 2, \ldots, n$ and they are not all zero. Since $(a_1''\boldsymbol{r}_1 + a_2''\boldsymbol{r}_2 + \cdots + a_n''\boldsymbol{r}_n) \bmod k_2 = \mathbf{0}$ by Eq. (3), $M \bmod k_2$ does not have property $\mathcal{J}_{k_2}$.

Conversely, assume that $M \bmod k_i$ does not have property $\mathcal{J}_{k_i}$ for $i = 1$ or $i = 2$. We may assume without loss of generality that $M \bmod k_1$ does not have property $\mathcal{J}_{k_1}$. Then, there exists $a_1, a_2, \ldots, a_n \in [k_1]$, not all zero, such that $(a_1\boldsymbol{r}_1 + a_2\boldsymbol{r}_2 + \cdots + a_n\boldsymbol{r}_n) \bmod k_1 = \mathbf{0}$. Since $k_2a_1, k_2a_2, \ldots, k_2a_n \in [k]$ and $(k_2a_1\boldsymbol{r}_1 + k_2a_2\boldsymbol{r}_2 + \cdots + k_2a_n\boldsymbol{r}_n) \bmod k = \mathbf{0}$, we conclude that M does not have property $\mathcal{J}_k$. $\blacksquare$

Corollary 2. *Let p be a prime and let l be a positive integer. Then, an $n \times n$ matrix M over $[p^l]$ has property $\mathcal{J}_{p^l}$ if and only if $M \bmod p$ has property $\mathcal{J}_p$.*

Proof. The proof is by induction on l using Lemma 8. $\blacksquare$

Corollary 3. *Let x be a positive integer and let $k = p_1^{l_1}p_2^{l_2} \cdots p_x^{l_x}$, where p_i is a prime and l_i is a positive integer for any i, $1 \leq i \leq x$. Then, an $n \times n$ matrix M over $[k]$ has property $\mathcal{J}_k$ if and only if $M \bmod p_i$ has property $\mathcal{J}_{p_i}$ for any $i = 1, 2, \ldots, x$.*

Proof. The proof is by induction on x using Corollary 2 and Lemma 8. $\blacksquare$

Theorem 9. *$\Lambda(1, n, k) = k^n$ for any integer $k \geq 3$.*

Proof. If M is the $(n + 1) \times n$ matrix obtained from I_n by adding a row consisting of 1's, then $G_p(M)$ is a 1-DFT matrix graph for $D_n(p)$ for any prime p. Thus, if M' is the matrix obtained from M by deleting any one row, then $G_p(M')$ is isomorphic to $D_n(p)$, and so M' has property $\mathcal{J}_p$ by Theorem 2. By Corollary 3, M' has property $\mathcal{J}_k$ for any positive integer $k \geq 3$, and so $G_k(M')$ is isomorphic to $D_n(k)$ by Theorem 2. Hence, $G_k(M)$ is a 1-DFT matric graph for $D_n(k)$, and $\Lambda(1, n, k) \leq k^n$.

If M is a $m \times n$ matrix such that $G_k(M)$ is a 1-DFT

matric graph for $D_n(k)$, then $m \geq n + 1$, and so $\Lambda(1, n, k) \geq k^n$. ■

Lemma 9. *Let p be a prime and let M be an $m \times n$ matrix over $GF(p)$. If $G_p(M)$ is a t-DFT matric graph for $D_n(p)$, then $G_{p^l}(M)$ is a t-DFT matric graph for $D_n(p^l)$, where l is a positive integer.*

Proof. If $G_p(M)$ is a t-DFT matric graph for $D_n(p)$, then, for any $S \subset R(M)$ with $|S| \leq t$, there exists some $S' \subset R(M) - S$ with $|S'| = m - n - |S|$ such that $G_p(M \backslash S \backslash S')$ is isomorphic to $D_n(p)$. Then, $M \backslash S \backslash S'$ has property $\mathcal{J}_p$ by Theorem 2, and so property $\mathcal{J}_{p^l}$ by Corollary 2. Thus, $G_{p^l}(M \backslash S \backslash S')$ is isomorphic to $D_n(p^l)$ by Theorem 2. Hence, $G_{p^l}(M)$ is a t-DFT matric graph for $D_n(p^l)$. ■

Theorem 10. *Let p be a prime and let l be a positive integer where $p^l \geq 3$. Then,*

$$\Lambda(t, n, p^l) \leq (t-1)p^{ln} \times \left\{ 2 \log_p \left(\frac{n}{t-1} + c_p \right) + c_p \right\} + p^{ln},$$

where $t \geq 2$ and $c_p = 1 + \log_p e$.

Proof. The proof is by Lemma 9 and Theorem 6. ■

Theorem III [10]. *Let n be an integer where $n \geq 2$, and let $p \geq n - 1$ be a prime. Then, there exists an $m \times n$ matrix M over $GF(p)$ such that $G_p(M)$ is a t-DFT matric graph for $D_n(p)$ and $m = n + t$ where $t \leq p + 1 - n$.*

Theorem 11. *Let p be a prime and let l be a positive integer where $p^l \geq 3$. Then,*

$$\Lambda(t, n, p^l) = tp^{ln},$$

where $t \leq p + 1 - n$.

Proof. By Lemma 9 and Theorem III, $\Lambda(t, n, p^l) \leq tp^{ln}$.

If M is a $m \times n$ matrix over $[p^l]$ such that $G_{p^l}(M)$ is a t-DFT matric graph for $D_n(p^l)$, then $m \geq n + t$, and so $\Lambda(t, n, p^l) \geq tp^{ln}$. ■

4. t-EFT GRAPHS FOR $D_n(k)$

Since a t-DFT matric graph for $D_n(k)$ is also a t-EFT graph for $D_n(k)$, we have $\Delta(t, D_n(k)) \leq \Lambda(t, n, k)$. Thus, we obtain Theorems 12, 13, and 14 from Theorems 9, 10, and 11, respectively.

Theorem 12. *$\Delta(1, D_n(k)) \leq k^n$ for any integer $k \geq 3$.* ■

Theorem 13. *Let p be a prime and let l be a positive integer where $p^l \geq 3$. Then,*

$$\Delta(t, D_n(p^l)) \leq (t-1)p^{ln} \times \left\{ 2 \log_p \left(\frac{n}{t-1} + c_p \right) + c_p \right\} + p^{ln},$$

where $t \geq 2$ and $c_p = 1 + \log_p e$. ■

Theorem 14. *Let p be a prime and let l be a positive integer where $p^l \geq 3$. Then,*

$$\Delta(t, D_n(p^l)) \leq tp^{ln},$$

where $t \leq p + 1 - n$. ■

On the other hand, we have the following lower bound:

$$\Delta(t, D_n(k)) \geq \tfrac{1}{2}tk^n, \tag{4}$$

since the degree of each vertex of a t-EFT graph for $D_n(k)$ is at least $2n + t$. It is an interesting open problem to close the gap between bounds in theorems above and (4).

The authors are grateful to Professor Y. Kajitani for his encouragement. The research is a part of the CAD21 Project at TIT.

REFERENCES

[1] M. Ajitai, N. Alon, J. Bruck, R. Cypher, C. T. Ho, and M. Naor, Fault tolerant graphs, perfect hash functions and disjoint paths. *Proceedings of the IEEE Symposium on Foundations of Computer Science* (1992) 693–702.

[2] N. Alon and F. R. K. Chung, Explicit construction of linear sized tolerant networks. *Discr. Math.* **72** (1988) 15–19.

[3] F. Annexstein, Fault tolerance in hypercube-derivative networks. *Proceedings of the ACM Symposium on Parallel Algorithms and Architectures* (1989) 179–188.

[4] B. Becker and H. U. Simon, How robust is the n-cube? *Info. Comput.* **77** (1988) 162–178.

[5] J. Bruck, R. Cypher, and C. T. Ho, Fault-tolerant meshes with minimal numbers of spares. *Proceedings of the 3rd IEEE Symposium on Parallel and Distributed Processing* (1991) 288–295.

[6] J. Bruck, R. Cypher, and C. T. Ho, Fault-tolerant meshes and hypercubes with minimal numbers of spares. *IEEE Trans. Comput.* (1993) 1089–1104.

[7] J. Bruck, R. Cypher, and C. T. Ho, Fault-tolerant meshes with small degree. *Proceedings of the ACM Symposium on Parallel Algorithms and Architectures* (1993) 1–10.

[8] J. Bruck, R. Cypher, and C. T. Ho, Fault-tolerant de Bruijn and shuffle-exchange networks. *IEEE Trans. Parallel Distrib. Syst.* **5** (1994) 548–553.

[9] J. Bruck, R. Cypher, and C. T. Ho, Tolerating faults in a mesh with a row of spare nodes. *Theor. Comput. Sci.* **128** (1994) 241–252.

[10] J. Bruck, R. Cypher, and C. T. Ho, Wildcard dimensions, coding theory and fault-tolerant meshes and hypercubes. *IEEE Trans. Comput.* **44** (1995) 150–155.

[11] J. Bruck, R. Cypher, and D. Soroker, Running algorithms efficiently on faulty hypercubes. *Proceedings of the ACM Symposium on Parallel Algorithms and Architectures* (1990) 37–44.

[12] J. Bruck, R. Cypher, and D. Soroker, Tolerating faults in hypercubes using subcube partitioning. *IEEE Trans. Comput.* **41** (1992) 599–605.

[13] J. Bruck and C. T. Ho, Fault-tolerant cube graphs and coding theory. Preprint (1995).

[14] A. A. Farrag and R. J. Dawson, Designing optimal fault-tolerant star networks. *Networks* **19** (1989) 707–716.

[15] A. A. Farrag and R. J. Dawson, Fault-tolerant extensions of complete multipartite networks. *Proceedings of the 9th International Conference on Distributed Computing Systems* (1989) 143–150.

[16] W. Feller, *An Introduction to Probability Theory and Its Applications.* Modern Asia Edition, 2 ed., **1** John Wiley & Sons, Inc., New York (1964).

[17] N. Graham, F. Harary, M. Livingston, and Q. F. Stout, Subcube fault-tolerance in hypercubes. *Info. Comput.* **102** (1993) 280–314.

[18] F. Harary and J. P. Hayes, Edge fault tolerance in graphs. *Networks* **23** (1993) 135–142.

[19] J. Hastad, F. T. Leighton, and M. Newman, Fast computations using faulty hypercubes. *Proceedings of the ACM Symposium on Theory of Computing* (1989) 251–284.

[20] J. P. Hayes, A graph model for fault-tolerant computing systems. *IEEE Trans. Comput.* **C-25** (1976) 875–883.

[21] C. T. Ho, An observation on the bisectional interconnection networks. *IEEE Trans. Comput.* **41** (1992) 873–877.

[22] C. Kaklamanis, A. R. Karlin, F. T. Leighton, V. Milenkovic, P. Raghavan, S. Rao, C. Thomborson, and A. Tsantilas, Asymptotically tight bounds for computing with faulty arrays of processors. *Proceedings of the IEEE Symposium on Foundations of Computer Science* (1990) 285–296.

[23] M. Paoli, W. W. Wong, and C. K. Wong, Minimum *k*-Hamiltonian graphs. *J. Graph Theory* **10** (1986) 79–95.

[24] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes,* 2nd ed. MIT Press, Cambridge, MA (1972).

[25] A. L. Rosenberg, Fault-tolerant interconnection networks, a graph theoretic approach. *Workshop on Graph-Theoritec Concepts in Computer Science, Trauner Veriag, Linz* (1983) 286–297.

[26] S. Ueno, A. Bagchi, S. L. Hakimi, and E. F. Schmeichel, On minimum fault-tolerant networks. *SIAM J. Discr. Math.* **6** (1993) 565–574.

[27] W. W. Wong and C. K. Wong, Minimum *k*-Hamiltonian graphs. *J. Graph Theory* **8** (1984) 155–165.

[28] T. Yamada, K. Yamamoto, and S. Ueno, Fault-tolerant graphs for hypercubes and tori. *Proceedings of the 28th HICSS* **II** (1995) 499–505.

[29] G. W. Zimmerman and A. H. Esfahanian, Chordal rings as fault-tolerant loops. *Discr. Appl. Math.* **37/38** (1992) 563–573.