[14] H-O. Peitgen, H. Jürgens, and D. Saupe, *Chaos and Fractals. New Frontiers of Science*. New York: Springer-Verlag, 1992.
[15] R. Rovatti, G. Setti, and G. Mazzini, "Chaotic complex spreading sequences for asynchronous DS-CDMA—Part II: Some theoretical performance bounds," *IEEE Trans. Circuits Syst. I*, vol. 45, pp. 496–506, Apr. 1998.
[16] M. R. Schroeder, *Number Theory in Science and Communication*. New York: Springer-Verlag, 1990.
[17] H. G. Schuster, *Deterministic Chaos. An Introduction*. Weinhem, Germany: VCH Verlagsgesellschaft , 1988.

Perfect r-Domination in the Kronecker Product of Three Cycles

Pranava K. Jha

***Abstract*—If $r \geq 1$, and m_0, m_1 and m_2 are each a multiple of $(r+1)^3 + r^3$, then each isomorphic component of the graph $C_{m_0} \times C_{m_1} \times C_{m_2}$ admits of a vertex partition into $(r+1)^3 + r^3$ perfect r-dominating sets. The result induces a dense packing of $C_{m_0} \times C_{m_1} \times C_{m_2}$ by means of vertex-disjoint subgraphs, each isomorphic to a connected component of $P_{2r+1} \times P_{2r+1} \times P_{2r+1}$. Additional results include a general lower bound on r-domination number of a Kronecker product of finitely many cycles. Areas of applications include efficient resource placement in communication networks and error-correcting codes.**

***Index Terms*—Cycle, error-correcting codes, graph theory, Kronecker product, perfect domination, resource placement, vertex partition.**

I. Introduction

Consider a computer/communication network that usually has a regular structure. The nodes are distinguishable into resource nodes and nonresource nodes. Each of the former houses replicable items such as power sources, I/O ports, function libraries and algorithmic information, while each of the latter is within a distance of r from at least one resource node, where $r \geq 1$. The resources are usually limited and expensive, hence the need for minimizing the number of respective nodes. An optimal solution is reached when each nonresource node is within a distance of r from exactly one resource node.

The foregoing problem of efficient resource placement has a natural graph-theoretical formulation, where the objective is to construct a *perfect r-dominating set* (formally defined below) of the underlying graph. It has been studied with respect to a number of network topologies, including hypercubes [1], 2-D torus [2] and 3-D torus [3]. The main result of this paper consists of a vertex partition of the *Kronecker product* (or $\times$*-product*, defined later) of three cycles into perfect r-dominating sets, where length of each cycle is a multiple of $(r+1)^3 + r^3$.

The concept of perfect r-domination has applications in several other areas, notably, error-correcting codes, game theory and frequency assignment [4]–[7]. The well-known Hamming code corresponds to a perfect 1-domination in the n-cube, where $n = 2^k - 1, k \geq 2$ [8], [9]. Even when a perfect r-dominating set is not known for a given graph, an analogous information with respect to a related graph may be useful to help construct a near-optimal set.

Manuscript received September 29, 2000; revised June 11, 2001. This paper was recommended by Associate Editor K. Thulasiraman.

The author is with the Department of Computer Science, St. Cloud State University, St. Cloud, MN 56301-4498 (e-mail: pkjha@eeyore.stcloudstate.edu).

Publisher Item Identifier S 1057-7122(02)00277-5.

Each connected component of $C_{m_0} \times C_{m_1} \times C_{m_2}$ is a regular graph of degree eight, has a low diameter [10], and is edge-decomposable into Hamiltonian cycles [11]. Accordingly, it is amenable to an application as a fault-tolerant communication network. The graph $C_{2i+1} \times C_{2j+1}$ has been called a diagonal mesh [12] that has proved to be useful in parallel computer architecture.

By a graph is meant a finite, simple and undirected graph. Unless indicated otherwise, graphs are also connected and contain at least two vertices. For $m \geq 2$ and $n \geq 3$, let P_m (resp. C_n) denote a *path* (resp. a *cycle*) on m (resp. n) vertices, where $V(P_k) = V(C_k) = \{0, \ldots, k-1\}$, and where adjacencies are defined in a natural way.

For a graph $G = (V, E)$, a vertex v is said to r-dominate a vertex w if $0 \leq d_G(v, w) \leq r$. A vertex subset S is called an *r-dominating set* (resp. a *perfect r-dominating set*) if every vertex of G is r-dominated by some vertex (resp. a unique vertex) in S. The cardinality of a smallest r-dominating set of G is called the *r-domination number* of G, denoted by $\gamma_r(G)$. It is easy to see that $\gamma_r(C_n) = \gamma_r(P_n) = \lceil n/(2r+1) \rceil$. The general problem of determining $\gamma_r(G)$ is known to be NP-hard even for bipartite graphs [13].

For graphs $G = (V, E)$ and $H = (W, F)$, the *Kronecker product* $G \times H$ of G and H is defined as follows: $V(G \times H) = V \times W$ and $E(G \times H) = \{\{(a, x), (b, y)\}: \{a, b\} \in E \text{ and } \{x, y\} \in F\}$. This product is variously known as direct product, cardinal product, categorical product, tensor product, and cross product. It is commutative and associative in a natural way, and is distributive with respect to edge-disjoint union of graphs. For any undefined terms or missing references, see the recent monograph by Imrich and Klavžar [14].

If G and H are not both bipartite, then $G \times H$ is connected, otherwise $G \times H$ consists of two connected components where vertices (a, x) and (b, y) belong to the same component if and only if $d_G(a, b)$ and $d_H(x, y)$ are of the same parity, where d_G denotes the (shortest) distance metric in G. Further $G \times H$ is bipartite if and only if G or H is bipartite. It is easy to see that the order of $G \times H$ is $|V| \cdot |W|$ and the size is $2 \cdot |E| \cdot |F|$. The following result will be useful in the sequel.

Proposition 1.1:

1) If G and H are both bipartite, and $(a, x), (b, y)$ belong to the same component of $G \times H$, then $d_{G \times H}((a, x), (b, y)) = \max\{d_G(a, b), d_H(x, y)\}$.
2) If G and H are both nonbipartite, then $\mathrm{og}(G \times H) = \max\{\mathrm{og}(G), \mathrm{og}(H)\}$, where $\mathrm{og}(G)$ denotes the odd girth, i.e., length of a shortest odd cycle of G.

■

For $m_0, \ldots, m_{k-1} \geq 3$, with $k \geq 2$, the following remarks are relevant [11]: (i) $C_{m_0} \times \cdots \times C_{m_{k-1}}$ is a regular graph of degree 2^k, and (ii) If the number of even integers among $m_0, \ldots, m_{k-1}$ is $p \geq 2$, then $C_{m_0} \times \cdots \times C_{m_{k-1}}$ consists of 2^{p-1} components that are mutually isomorphic.

Perfect r-dominating sets with respect to the Cartesian product $C_{m_0} \square \cdots \square C_{m_{k-1}}$ and (each component of) the Kronecker product $C_{m_0} \times \cdots \times C_{m_{k-1}}$ are known for certain cases. See Table I. Domination in the Kronecker product, in general, has been studied by several authors [18]–[20].

Section II presents a lower bound on $\gamma_r(C_{m_0} \times \cdots \times C_{m_{k-1}})$ and shows that the subgraph induced by vertices within a distance of r from a particular vertex of $C_{m_0} \times \cdots \times C_{m_{k-1}}$ is isomorphic to a connected component of the $\times$-product of k copies of P_{2r+1}. Section III presents the main result, and a corollary dealing with: 1) exact value of $\gamma_r(C_{m_0} \times C_{m_1} \times C_{m_2})$ and 2) a dense packing of $C_{m_0} \times C_{m_1} \times C_{m_2}$ by means of vertex-disjoint subgraphs isomorphic to a connected component of $P_{2r+1} \times P_{2r+1} \times P_{2r+1}$, where m_0, m_1 and m_2 are each a multiple of $(r+1)^3 + r^3$.

1057–7122/02$17.00 © 2002 IEEE

Authorized licensed use limited to: SAINT CLOUD STATE UNIVERSITY. Downloaded on May 03,2010 at 19:32:10 UTC from IEEE Xplore. Restrictions apply.

TABLE I
EXISTENCE OF PERFECT r-DOMINATING SETS IN PRODUCTS OF CYCLES

$C_{m_0} \Box \cdots \Box C_{m_{k-1}}$	$C_{m_0} \times \cdots \times C_{m_{k-1}}$
$r = 1$, $k \geq 1$ and $m_0, \cdots, m_{k-1}$ each a multiple of $2k+1$ [4, 15]	$r = 1$, $k \geq 2$ and $m_0, \cdots, m_{k-1}$ each a multiple of $2^k + 1$ [16]
$r \geq 1$, $k = 2$ and m_0, m_1 each a multiple of $2r^2 + 2r + 1$ [4, 15]	$r \geq 1$, $k = 2$ and m_0, m_1 each a multiple of $2r^2 + 2r + 1$ [17]

II. PRELIMINARIES

Definition 1: Let G be a graph with radius s. For $0 \leq r \leq s$, an r-ball centered at a vertex v of G is the set $\{w \in V(G) : 0 \leq d_G(v, w) \leq r\}$. ■

An r-dominating set of G is a spanning of G by r-balls [15]. In the case of a perfect r-dominating set, the r-balls are mutually exclusive and exhaustive. In what follows, an "r-ball" will be used also to denote the corresponding induced subgraph.

Lemma 2.1: For $r \geq 1$ and $k \geq 2$, let $m_0, \ldots, m_{k-1} \geq 2r + 2$. The order of an r-ball in $C_{m_0} \times \cdots \times C_{m_{k-1}}$ is equal to $(r+1)^k + r^k$ while the size is equal to $(2r)^k$.

Proof: Since $m_0, \ldots, m_{k-1} > 2r + 1$, an r-ball in $C_{m_0} \times \cdots \times C_{m_{k-1}}$ is necessarily bipartite, cf. Proposition 1.1(2).

Let $(v_0, \ldots, v_{k-1}) \in V(C_{m_0} \times \cdots \times C_{m_{k-1}})$. For $1 \leq p \leq r$, a vertex at a distance of p from $(v_0, \ldots, v_{k-1})$ is of the form $(v_0 + a_0, \ldots, v_{k-1} + a_{k-1})$, where

- $a_0, \ldots, a_{k-1} \in \{-p + 2j : 0 \leq j \leq p\}$;
- $\max\{|a_0|, \ldots, |a_{k-1}|\} = p$;
- $v_i + a_i$ is modulo $m_i, 0 \leq i \leq k-1$.

Thus, vertices at a distance of p from $(v_0, \ldots, v_{k-1})$ total $(p+1)^k - (p-1)^k$. Accordingly, the order of an r-ball is equal to

$$1 + \sum_{p=1}^{r} ((p+1)^k - (p-1)^k) = (r+1)^k + r^k.$$

Observe next that an r-ball may be viewed as a (sub)graph consisting of levels $0, \ldots, r$, where $(v_0, \ldots, v_{k-1})$ is the sole resident of level 0, and vertices at level p are of the form $(v_0 + a_0, \ldots, v_{k-1} + a_{k-1})$, where $a_0, \ldots, a_{k-1}$ are as mentioned earlier. Since an r-ball itself is bipartite, vertices at the same level are necessarily nonadjacent.

Note that every vertex of $C_{m_0} \times \cdots \times C_{m_{k-1}}$ is of degree 2^k. Accordingly, every vertex in an r-ball up to level $r-1$ is of degree 2^k. It is claimed that the number of edges between level p and level $p+1$ is equal to $2^k \cdot ((p+1)^k - p^k)$, where $0 \leq p \leq r-1$. For $p = 0$, the claim is easily seen to be true. Let $p \geq 1$. There are a total of $(p+1)^k - (p-1)^k$ mutually nonadjacent vertices at level p, and hence there are a total of $2^k \cdot ((p+1)^k - (p-1)^k)$ edges incident on them. Out of these, $2^k \cdot (p^k - (p-1)^k)$ are between level $p-1$ and level p (by induction hypothesis). Thus the number of edges between level p and level $p+1$ is equal to

$$2^k \cdot ((p+1)^k - (p-1)^k) - 2^k \cdot (p^k - (p-1)^k) = 2^k \cdot ((p+1)^k - p^k).$$

By the foregoing claim, the size of an r-ball is given by

$$\sum_{p=0}^{r-1} \left(2^k \cdot ((p+1)^k - p^k)\right) = 2^k \cdot r^k = (2r)^k.$$

■

The following lower bound is immediate.

Lemma 2.2:

$$\gamma_r(C_{m_0} \times \cdots \times C_{m_{k-1}}) \geq \frac{\Pi_{i=0}^{k-1} m_i}{(r+1)^k + r^k}.$$

■

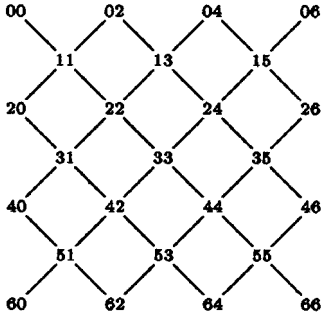

Fig. 1. The graph $P_7^2(0)$.

As stated in Table I, and subsequently in Corollary 3.2(1), the lower bound of Lemma 2.2 is achievable in certain cases.

Let $k \geq 2$, and consider the graph $P_{2r+1}^k = P_{2r+1} \times \cdots \times P_{2r+1}$ (k factors) that consists of 2^{k-1} connected components (all bipartite) where vertices $(v_0, \ldots, v_{k-1})$ and $(w_0, \ldots, w_{k-1})$ belong to the same component if and only if $v_i + v_{i+1}$ and $w_i + w_{i+1}$ are of the same parity, $0 \leq i \leq k-2$. Let $P_{2r+1}^k(0)$ denote the connected component that includes the vertex $(0, \ldots, 0)$, i.e., k-tuple of all 0's. It is shown in the rest of the section that an r-ball in $C_{m_0} \times \cdots \times C_{m_{k-1}}$ is isomorphic to $P_{2r+1}^k(0)$. The following remarks are relevant.

1) The two partite sets of $P_{2r+1}^k(0)$ are given by:
   - $V_0 = \{(v_0, \ldots, v_{k-1})$: v_i is an even integer between 0 and $2r\}$.
   - $V_1 = \{(w_0, \ldots, w_{k-1})$: w_i is an odd integer between 1 and $2r-1\}$.
2) $P_{2r+1}^k(0)$ is unique among all connected components of P_{2r+1}^k in that all pendant vertices of P_{2r+1}^k are included in it. (Pendant vertices are those $(v_0, \ldots, v_{k-1})$ in which each v_i is either 0 or $2r$.)

Note that $|V_0| = (r+1)^k$ and $|V_1| = r^k$, hence the order of $P_{2r+1}^k(0)$ is $(r+1)^k + r^k$. Also, size of $P_{2r+1}^k(0)$ is $(2r)^k$, which follows from the fact that if G and H are bipartite graphs, then the size of each connected component of $G \times H$ is equal to $|E(G)| \cdot |E(H)|$. Graph $P_7^2(0)$ appears in Fig. 1; for simplicity, vertices (i, j) have been shown as ij.

Observe that the order (respective size) of $P_{2r+1}^k(0)$ coincides with the order (resp. size) of an r-ball in $C_{m_0} \times \cdots \times C_{m_{k-1}}$, where $m_0, \ldots, m_{k-1} \geq 2r + 2$. The two graphs are actually isomorphic. To see this, let $\bar{r} = (r, \ldots, r)$, i.e., k-tuple of all r's. It is easy to see that $\bar{r}$ belongs to $P_{2r+1}^k(0)$ and is such that (i) every vertex is within a distance of r from $\bar{r}$, and (ii) no other vertex has this property. In other words, $\bar{r}$ is the unique center of $P_{2r+1}^k(0)$. (Vertices $(w_0, \ldots, w_{k-1})$ at a distance of exactly r from $\bar{r}$ are such that at least one w_i is 0 or $2r$.)

Analogous to the structure of an r-ball, $P_{2r+1}^k(0)$ may be viewed as a graph consisting of levels $0, \ldots, r$, where $\bar{r} = (r, \ldots, r)$ is the sole resident of level 0, and vertices at level p are of the form $(r + a_0, \ldots, r + a_{k-1})$ where $a_0, \ldots, a_{k-1}$ are as in the proof of Lemma 2.1. The reader may check to see that there is a natural bijection $(v_0 + a_0, \ldots, v_{k-1} + a_{k-1}) \leftrightarrow (r + a_0, \ldots, r + a_{k-1})$ between the vertex

Authorized licensed use limited to: SAINT CLOUD STATE UNIVERSITY. Downloaded on May 03,2010 at 19:32:10 UTC from IEEE Xplore. Restrictions apply.

TABLE II
VARIOUS CASES

1.	$a = p$	$0 \le b \le p$	$0 \le c \le p$
2.	$a = p$	$0 \le b \le p$	$-p \le c < 0$
3.	$a = p$	$-p \le b < 0$	$0 \le c \le p$
4.	$a = p$	$-p \le b < 0$	$-p \le c < 0$
5.	$0 \le a \le p$	$b = p$	$0 \le c \le p$
6.	$0 \le a \le p$	$b = p$	$-p \le c < 0$
7.	$0 \le a \le p$	$b = -p$	$0 \le c \le p$
8.	$0 \le a \le p$	$b = -p$	$-p \le c < 0$
9.	$0 \le a \le p$	$0 \le b \le p$	$c = p$
10.	$0 \le a \le p$	$-p \le b < 0$	$c = p$
11.	$0 \le a \le p$	$0 \le b \le p$	$c = -p$
12.	$0 \le a \le p$	$-p \le b < 0$	$c = -p$

set of the r-ball centered at $(v_0 + a_0, \ldots, v_{k-1} + a_{k-1})$ and the vertex set of $P^k_{2r+1}(0)$ (centered at $\bar{r}$) that corresponds to an isomorphism.

Lemma 2.3: For $r \ge 1$ and $k \ge 2$, if $m_0, \ldots, m_{k-1} \ge 2r + 2$, then an r-ball in $C_{m_0} \times \cdots \times C_{m_{k-1}}$ is isomorphic to $P^k_{2r+1}(0)$. ■

III. MAIN RESULT

The following is the central result of this paper.

Theorem 3.1: For $r \ge 1$, if m_0, m_1 and m_2 are each a multiple of $(r+1)^3 + r^3$, then each isomorphic component of $C_{m_0} \times C_{m_1} \times C_{m_2}$ admits of a vertex partition into $(r + 1)^3 + r^3$ perfect r-dominating sets.

Proof: Let $n = (r + 1)^3 + r^3 = 2r^3 + 3r^2 + 3r + 1$, and let a typical vertex (v_0, v_1, v_2) of $C_{m_0} \times C_{m_1} \times C_{m_2}$ be assigned the integer label

$$(2((r + 1)^2 + r^2)v_0 + 2(r + 1)v_1 + 2rv_2) \bmod n.$$

The assignment is clearly well-defined. It suffices to show that a vertex distinct from (v_0, v_1, v_2) and within a distance of $2r$ from (v_0, v_1, v_2) receives a label that is different from that of (v_0, v_1, v_2).

Let $p \in \{1, \ldots, 2r\}$, and consider a vertex at a distance of p from (v_0, v_1, v_2). Such a node is of the form $(v_0 + a, v_1 + b, v_2 + c)$, where (i) $a, b, c \in \{-p + 2j : 0 \le j \le p\}$, (ii) $\max\{|a|, |b|, |c|\} = p$, and (iii) $v_0 + a$ is modulo m_0; $v_1 + b$ is modulo m_1; and $v_2 + c$ is modulo m_2. (Note that a, b and c are of the same parity.) The label assigned to $(v_0 + a, v_1 + b, v_2 + c)$ is

$$(2((r + 1)^2 + r^2)v_0 + 2(r + 1)v_1 + 2rv_2 + 2((r + 1)^2 + r^2)a + 2(r + 1)b + 2rc) \bmod n.$$

That this label is different from the one assigned to (v_0, v_1, v_2) is equivalent to

$$(2((r + 1)^2 + r^2)a + 2(r + 1)b + 2rc) \bmod n > 0.$$

For integers s and t, where t is odd ≥ 3, it is easy to see that $(2s) \bmod t = x > 0$ if and only if $(-2s) \bmod t = t - x > 0$. Based on this fact, it suffices to prove the stated claim for $a \ge 0$. Accordingly, there are a total of twelve cases, as detailed in Table II.

The reader may check to see that

- $2((r+1)^2 + r^2)a + 2(r+1)b + 2rc$ is of the form $4t$ for some t, where a, b and c are of the same parity;
- $2((r+1)^2 + r^2)a + 2(r+1)b + 2rc$ is strictly between $-2n$ and $5n$ for $0 \le a \le 2r$; $-2r \le b \le 2r$; and $-2r \le c \le 2r$.

Based on these observations, it need only be shown that $2((r+1)^2 + r^2)a + 2(r+1)b + 2rc$, i.e., $2 \cdot [(2r^2+2r+1)a + (r+1)b + rc]$ is nonzero and not equal to $4n = 4(2r^3 + 3r^2 + 3r + 1) = 2 \cdot [4r^3 + 6r^2 + 6r + 2]$. In other words, the following claims need to be established for each of the twelve cases.

1) $(2r^2 + 2r + 1)a + (r + 1)b + rc \ne 0$, and
2) $(2r^2 + 2r + 1)a + (r + 1)b + rc \ne 4r^3 + 6r^2 + 6r + 2$.

Case 1: $a = p, 0 \le b \le p$ and $0 \le c \le p$.

First note that $(2r^2 + 2r + 1)a + (r + 1)b + rc$, i.e., $(2r^2 + 2r + 1)p + (r+1)b + rc$ is clearly positive, and hence nonzero. Assume that

$$(2r^2 + 2r + 1)p + (r + 1)b + rc = 4r^3 + 6r^2 + 6r + 2, \text{ i.e.,}$$
$$2pr^2 + (2p + b + c)r + (p + b) = 4r^3 + 6r^2 + 6r + 2, \text{ i.e.,}$$
$$(pr + p + 1/2(b+c)) \cdot (2r) + (p+b) = (2r^2 + 3r + 3) \cdot (2r) + 2.$$

Note that b and c being of the same parity, $b + c$ is even. For the foregoing equality to hold, $(p+b) \equiv 2$ modulo $(2r)$. Since $0 < p+b \le 4r$, either $p + b = 2$ or $p + b = 2r + 2$. If $p + b = 2$, then $p \le 2$ and hence $c \le 2$, in which case $2pr^2 + (2p + b + c)r + (p + b)$ is at most $4r^2 + 6r + 2 < 4r^3 + 6r^2 + 6r + 2$. On the other hand, if $p + b = 2r + 2$, then $2pr^2 + (2p + b + c)r + (p + b)$ is at most $(4r) \cdot r^2 + (2r + 2r + 2 + 2r) \cdot r + (2r + 2) = 4r^3 + 6r^2 + 4r + 2 < 4r^3 + 6r^2 + 6r + 2$. Contradiction.

Case 2: $a = p, 0 \le b \le p$ and $-p \le c < 0$.

Let $c = -e$ whence $0 < e \le p$, and note that $(2r^2 + 2r + 1)a + (r + 1)b + rc = (2r^2 + 2r + 1)p + (r + 1)b - re$ that is clearly positive, since $p \ge 1$ and $2r^2 + 2r + 1 > 2r^2 \ge re$. Further, $(2r^2 + 2r + 1)p + (r+1)b - re < (2r^2 + 2r + 1)p + (r+1)b \le (2r^2 + 2r + 1) \cdot (2r) + (r + 1) \cdot (2r) = 4r^3 + 6r^2 + 4r < 4r^3 + 6r^2 + 6r + 2$.

Case 3: $a = p, -p \le b < 0$ and $0 \le c \le p$.

Let $b = -d$ whence $0 < d \le p$, and note that $(2r^2 + 2r + 1)a + (r + 1)b + rc = (2r^2 + 2r + 1)p - (r + 1)d + rc$ that is clearly positive, hence nonzero. Further, $(2r^2 + 2r + 1)p - (r + 1)d + rc < (2r^2 + 2r + 1)p + rc \le (2r^2 + 2r + 1) \cdot (2r) + r \cdot (2r) = 4r^3 + 6r^2 + 2r < 4r^3 + 6r^2 + 6r + 2$.

Case 4: $a = p, -p \le b < 0$ and $-p \le c < 0$.

Let $b = -d$ and $c = -e$ whence $0 < d, e \le p$, and note that $(2r^2 + 2r + 1)a + (r + 1)b + rc$, i.e., $(2r^2 + 2r + 1)p - (r + 1)d - re$ is positive, since $p \ge 1; p \ge d, e$ and $2r^2 + 2r + 1 > r + 1 + r$. Further, it is easy to see that $(2r^2 + 2r + 1)p - (r + 1)d - re < 4r^3 + 6r^2 + 6r + 2$.

Case 5: $0 \le a \le p, b = p$ and $0 \le c \le p$.

Argument is similar to that in Case 1.

Case 6: $0 \le a \le p, b = p$ and $-p \le c < 0$.

Argument is similar to that in Case 2.

Case 7: $0 \le a \le p, b = -p$ and $0 \le c \le p$.

$(2r^2 + 2r + 1)a + (r + 1)b + rc = (2r^2 + 2r + 1)a - (r + 1)p + rc$. If $a = 0$, then this expression is strictly negative, and if $a \ge 1$, then its least value is at least $(2r^2 + 2r + 1) - (r + 1) \cdot (2r) = 1$ corresponding to $a = 1, p = 2r$ and $c = 0$. It follows that $(2r^2 + 2r + 1)a - (r + 1)p + rc \ne 0$. That it is not equal to $4r^3 + 6r^2 + 6r + 2$ follows by an argument as in Case 3.

Case 8: $0 \le a \le p, b = -p$ and $-p \le c < 0$.

Let $c = -e$ whence $0 < e \le p$, and $(2r^2 + 2r + 1)a + (r + 1)b + rc = (2r^2 + 2r + 1)a - (r + 1)p - re$. Assume that

$$(2r^2 + 2r + 1)a - (r + 1)p - re = 0, \text{ i.e.,}$$
$$2ar^2 + (2a - p - e)r + (a - p) = 0, \text{ i.e.,}$$
$$(ar + a - 1/2(p + e)) \cdot (2r) + (a - p) = 0.$$

Note that p and e being of the same parity, $p + e$ is even. For the foregoing equality to hold, either $(a - p) = 0$ or $(a - p) = -2r$, since $0 \le a \le p \le 2r$. First suppose that $a - p = 0$, i.e., $a = p$ whence $2ar^2 + (2a - p - e)r + (a - p) = 2pr^2 + (p - e)r$ that is clearly positive, hence nonzero. Next suppose that $a - p = -2r$ which is possible if and only if $a = 0$ and $p = 2r$, whence $2ar^2 + (2a - p - e)r + (a - p) = (-2r - e)r - 2r$ that is clearly negative, hence nonzero. Contradiction. That $2ar^2 + (2a - p - e)r + (a - p)$ is strictly less than $4r^3 + 6r^2 + 6r + 2$ is easy to see.

Case 9: $0 \le a \le p, 0 \le b \le p$ and $c = p$.

Authorized licensed use limited to: SAINT CLOUD STATE UNIVERSITY. Downloaded on May 03,2010 at 19:32:10 UTC from IEEE Xplore. Restrictions apply.

Argument is similar to that in Case 1.

Case 10: $0 \le a \le p, -p \le b < 0$ and $c = p$.

Left to the reader.

Case 11: $0 \le a \le p, 0 \le b \le p$ and $c = -p$.

Left to the reader.

Case 12: $0 \le a \le p - p \le b < 0$ and $c = -p$.

Left to the reader.

In all of the foregoing arguments, the modulo arithmetic works correctly, since m_0, m_1 and m_2 are each a multiple of $n = (r+1)^3 + r^3$.

For (an isomorphic component of) $C_{m_0} \times C_{m_1} \times C_{m_2}$, let V_t denote the set of vertices that receive the label t, where $0 \le t \le n-1$. The sets $V_0, \ldots, V_{n-1}$ constitute a vertex partition into perfect r-dominating sets. ■

Results 2.1, 2.2, 3.1 together with the discussion in Section II lead to the following.

Corollary 3.2: Let $r \ge 1$, and let m_0, m_1 and m_2 each be a multiple of $(r+1)^3 + r^3$.

1)
$$\gamma_r\left(C_{m_0} \times C_{m_1} \times C_{m_2}\right) = \frac{m_0 m_1 m_2}{(r+1)^3 + r^3}.$$

2) $C_{m_0} \times C_{m_1} \times C_{m_2}$ admits of a vertex partition into $(m_0 m_1 m_2)/((r+1)^3 + r^3)$ induced subgraphs, each isomorphic to $P^3_{2r+1}(0)$.

■

Corollary 3.2(2) may be viewed as a packing of $C_{m_0} \times C_{m_1} \times C_{m_2}$ by means of $(m_0 m_1 m_2)/((r+1)^3 + r^3)$ vertex-disjoint (and hence edge-disjoint) copies of $P^3_{2r+1}(0)$, that has $(2r)^3$ edges. All such copies thus collectively account for $8r^3 \cdot (m_0 m_1 m_2/((r+1)^3 + r^3))$ edges of $C_{m_0} \times C_{m_1} \times C_{m_2}$ that has a total of $4m_0 m_1 m_2$ edges. Thus, the "density" of this packing is equal to

$$\frac{1}{4m_0 m_1 m_2} \cdot \left(8r^3 \cdot \frac{m_0 m_1 m_2}{(r+1)^3 + r^3}\right) = \frac{2r^3}{(r+1)^3 + r^3}$$

that approaches 100% for large r.

ACKNOWLEDGMENT

The author would like to thank the referee whose perceptive comments led to an improvement in the presentation of the paper.

REFERENCES

[1] H. Chen and N. Tzeng, "Efficient resource placement in hypercubes using multiple-adjacency codes," *IEEE Trans. Comput.*, vol. 43, pp. 23–33, Jan. 1994.

[2] M. Bae and B. Bose, "Resource placement in torus-based networks," *IEEE Trans. Comput.*, vol. 46, pp. 1083–1092, Oct. 1997.

[3] H. Choo, S.-M. Yoo, and H. Y. Youn, "Processor scheduling and allocation for 3D torus multicomputer systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 11, pp. 475–484, May 2000.

[4] S. W. Golomb and L. R. Welch, "Perfect codes in the Lee metric and the packing of polyominoes," *SIAM J. Appl. Math.*, vol. 18, no. 2, pp. 302–317, 1970.

[5] T. W. Haynes, S. T. Hedetniemi, and P. J. Slater, *Fundamentals of Domination in Graphs*. New York: Marcel-Dekker, 1998.

[6] J. Kratochvil, "Perfect codes over graphs," *J. Combin. Theory, Ser. B*, vol. 40, pp. 224–228, 1986.

[7] M. Livingston and Q. F. Stout, "Perfect dominating sets," *Congr. Numer.*, vol. 79, pp. 187–203, 1990.

[8] P. K. Jha and G. Slutzki, "A scheme to construct distance-three codes using latin squares, with applications to the n-cube," *Inform. Process. Lett.*, vol. 55, no. 3, pp. 123–127, 1995.

[9] V. Pless, *Introduction to the Theory of Error-Correcting Codes*, 2nd ed. New York: Wiley, 1989.

[10] S.-R. Kim, "Centers of a tensor-composite graph," *Congr. Numer.*, vol. 81, pp. 193–204, 1991.

[11] P. K. Jha, "Hamiltonian decompositions of products of cycles," *Indian J. Pure Appl. Math.*, vol. 23, no. 10, pp. 723–729, 1992.

[12] K. W. Tang and S. A. Padubirdi, "Diagonal and toroidal mesh networks," *IEEE Trans. Comput.*, vol. 43, pp. 815–826, July 1994.

[13] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*. New York: Freeman, 1979.

[14] W. Imrich and S. Klavžar, *Product Graphs: Structure and Recognition*. New York: Wiley , 2000.

[15] S. Gravier and M. Mollard, "On domination numbers of Cartesian products of paths," *Discrete Appl. Math.*, vol. 80, no. 2/3, pp. 247–250, 1997.

[16] P. K. Jha, "Smallest independent dominating sets in Kronecker products of cycles," *Discrete Appl. Math.*, submitted for publication.

[17] ——, Perfect r-domination in Kronecker product of cycles, with an application to diagonal/toroidal mesh, , June 2000. Manuscript.

[18] S. Gravier and A. Khelladi, "On the domination number of cross products of graphs," *Discrete Math.*, vol. 145, no. 1/3, pp. 273–277, 1995.

[19] S. Klavžar and B. Zmazek, "On a vizing-like conjecture for direct-product graphs," *Discrete Math.*, vol. 156, no. 1/3, pp. 243–246, 1996.

[20] A. Klobucar and N. Seifter, "k-dominating sets of cardinal products of paths," *Ars Combin.*, vol. 55, pp. 33–41, 2000.

A Note on Chaotic Secure Communication Systems

Zhong-Ping Jiang

***Abstract*—This paper presents a new way to transmit and retrieve an information-bearing signal via chaotic systems. In contrast to existing schemes with one transmission line, a *two-channel* transmission method is adopted for the purpose of faster synchronization and higher security. Basically, an output of the chaotic transmitter is sent for synchronization-only, with no connection to the information signal. The other channel transmits a signal generated from a highly nonlinear function of the chaotic states and the information-bearing signal. While the first channel serves the purpose of efficient synchronization, the second channel is used for complicated encryption and, therefore, improved security/privacy. Simulation results validate the new chaos-based secure communication method.**

***Index Terms*—Chaos synchronization, encryption, observer, secure communication.**

I. INTRODUCTION

Undoubtedly, data security has been a topic of increasing importance in communications as the Internet and personal communications systems are being made accessible worldwide. In recent years, using chaotic signals to address the secure communication problem has received a great deal of attention. Various methods for chaos-based secure transmission of private information signals have been proposed by several authors; see [12], [3], [6], [2], [1], [8], [15]–[17] and references therein. Some popular methods are additive masking, chaotic

Manuscript received January 28, 2001; revised May 15, 2001 and August 6, 2001. This work was supported in part by the U.S. National Science Foundation under Grant INT-9987317, Grant ANI-0081527, and Grant ECS-0093176. This paper was recommended by Associate Editor T. Saito.

The author is with the Department of Electrical and Computer Engineering, Polytechnic University, Brooklyn, NY 11201 USA (e-mail: zjiang@control.poly.edu).

Publisher Item Identifier S 1057-7122(02)00288-X.

1057–7122/02$17.00 © 2002 IEEE

Authorized licensed use limited to: SAINT CLOUD STATE UNIVERSITY. Downloaded on May 03,2010 at 19:32:10 UTC from IEEE Xplore. Restrictions apply.