In Congressus Numerantium 97 (1993), pp. 51-70.

Perfect Dominating Sets on Cube-Connected Cycles

Douglas Van Wieren

Marilynn Livingston

Quentin F. Stout

Advanced Computer Architecture Laboratory Electrical Engineering and Computer Science University of Michigan, Ann Arbor

Abstract

Cube-connected cycles are a family of cubic graphs with relatively small diameters and regular structure, making them attractive models for parallel architecture design. The existence of perfect dominating sets for any structural model of parallel computation is both useful for the construction of efficient algorithms for that structure and indicative of practical design constraints. This paper gives a simple algorithmic method for constructing perfect dominating sets on cube-connected cycles where they exist, and proves nonexistence for all other cases. Specifically, standard perfect dominating sets (distance equal to 1) are shown to exist for cube-connected cycles of order k, k not equal to 5. Moreover, the existence of perfect dominating sets for all distances greater than 1 is disproved (with the trivial exception — the distance equaling or exceeding the diameter of the graph).

Keywords: Cube-Connected Cycles, Dominating Sets, Perfect Dominating Sets, Parallel Architecture, Parallel Algorithms.

1 Notation and Background

1.1 Cube-connected cycles

Formally, a cube-connected cycle of order k^{-1} (here denoted \mathbf{CCC}_k) can be described as the labeled graph (V, E) where V, the vertices of \mathbf{CCC}_k , is the set

$$\left\{(i,j): i \in \{0,\ldots,k-1\}, j \in \left\{0,\ldots,2^{k}-1\right\}\right\}$$

and E, the edges of CCC_k , is the set of unordered pairs $\{(i_1, j_1), (i_2, j_2)\}$ where (i_1, j_1) and (i_2, j_2) are elements of V which satisfy either

$$i_1 + 1 \equiv i_2 \pmod{k}$$
 and $j_1 = j_2$
or
 $i_1 = i_2$ and $|j_1 - j_2| = 2^{(k-i_1-1)}$

The edges which satisfy the first condition are referred to as *cycle edges*; the remaining edges, exactly those which satisfy the second condition $(i_1 = i_2 \text{ and } |j_1 - j_2| = 2^{(k-i_1-1)})$, are referred to hypercube edges.

¹Cube-connected cycles of orders smaller than 3 are traditionally ignored in the same manner that cycles of order smaller than 3 are ignored. However, various reasonable extensions of the definition (i.e. nonsimple graphs) will produce graphs small enough to allow most results (including this one) to shown by inspection.

By inspection, the removal of all hypercube edges produces a graph with 2^k components, each of which is a *k*-cycle. Thus, contracting all the cycle edges in \mathbf{CCC}_k will produce a graph with 2^k vertices (in fact, a hypercube). For this reason, each *k*-cycle in \mathbf{CCC}_k which does not include any hypercube edges is referred as a *supervertex* of the (embedded) hypercube. Moreover, the *origin* of \mathbf{CCC}_k is the *set* of vertices in the supervertex located at 0.

In essence, the formal definition uniquely describes each vertex in \mathbf{CCC}_k by its position within the supervertex (the cycle *index*) and by the position of the the supervertex within the hypercube. Following the conventions established for the hypercube, the position of a supervertex will be described as a binary string (e.g. 010000000 or, in the form of a regular expression, $010^{(7)}$). Specific vertices will be described with the addition of an accent over the bit position corresponding to the index. (For simplicity, the bit positions will indexed from 0 to k - 1 from left to right.) An example of a cube-connected cycle and the notation used here is shown in figure 1. Informally, two vertices are adjacent if *either* they are located in the same supervertex and the corresponding indices are adjacent in the k-cycle or they each have the same cycle index and have supervertex locations which differ only in the bit position indicated by the index (accent). It follows that, for any k, each vertex in \mathbf{CCC}_k has degree 3, and, with this notation, the three neighbors can be described simply — e.g., in \mathbf{CCC}_6 , 101011 has neighbors, 101011, 101011, and 101001.



Figure 1: Cube-Connected Cycle of order 3

From the informal definition, it should be intuitive that, for any vertices v_0 and v_1 in \mathbf{CCC}_k , there exists a graph isomorphism which sends v_0 to v_1 — rotation or reversal of the dimensions (and corresponding cycle indices) and/or reflection over any dimension as needed.

A perfect dominating set of distance d (here abbreviated PDS_d) is a subset of the vertices of graph such

that every vertex in the graph is dominated by exactly one vertex in the set. Formally, for any graph G, let d(v, w) be the minimal path distance between the vertices v and w (with d(v, v) = 0). For a given positive integer distance d, a vertex v is said to *cover* or *dominate* w if and only if $d(v, w) \leq d$. Letting V(G) denote the set of vertices of G, a subset X of V(G) is a *dominating* set with distance d if and only if $\forall v \in V(G), \exists w \in X$ such that w covers v. A subset X of V(G) is a *perfect* dominating set with distance d if and only if $\forall v \in V(G), \exists u \in X$ such that w covers v. A subset X of V(G) is a *perfect* dominating set with distance d if and only if $\forall v \in V(G), \exists a unique w \in X$ such that w covers v. A standard perfect dominating set ² is a perfect dominating set of distance 1; an example of a standard perfect set is shown in table 1 and figure refpds3.

1.2 Motivation and Background

Cube-connected cycles, as mathematical structures, are interesting in and of themselves; however, they have two properties which make them particularly attractive as potential structures for massively parallel computers.

First, like the mesh, but unlike the hypercube, each node has a small, fixed degree. This allows the redesign of larger systems without the need to redesign and rethink the individual processors. Also, from the viewpoint of theoretical computer science, asymptotic analysis of hypercube algorithms holds troubling questions regarding the computational power of processors which have $\theta(\log n)$ connections.

Second, like the hypercube, but unlike the mesh, the diameter of the graph grows slowly with respect to the number of processors ($\theta(\log n)$ as opposed to $\theta(\sqrt{n})$). Since algorithms designed for parallel architectures often require data from all processors, reduction of the worst-case communication time may be a matter of necessity.

Dominating sets are also an area of strong concern in the design of both parallel structures and parallel algorithms. With a specified processor structure (such as the mesh, hypercube, or cube-connected cycle), it is often necessary to find an efficient method of distributing limited or costly replicable items — power sources, i/o ports, function libraries, algorithm information, etc. — among the processors. In some variations of the problem, resources may conflict, and, in fact, with regular structures, having resources placed within some (short) distance of every node is not always sufficient. Other considerations – such as the complexity of the paths between each processor and its designated resource – are also considerations. Because of regularity of the structures, a perfect dominating set is usually the best answer.

The existence of perfect dominating sets for the mesh family of architectures is fairly straightforward (depending on the mesh) and the hypercube has been investigated exhaustively for this property however, results for the cube-connected cycle architecture were not generally known beyond k > 12 and d > 1. Here, an algorithmic method is shown for constructing a **PDS**_d on **CCC**_k when d = 1 and $k \neq 5$. The nonexistence of nontrivial perfect dominating sets when d > 1 is also demonstrated.

2 Algorithmic Construction of Standard Perfect Dominating Sets

The existence of perfect dominating sets for d = 1 and $k \neq 5$ will be shown by explicit construction. In addition to describing the vertices which belong to this set, it will also be useful to distinguish between the non-member vertices by the direction in which the vertex which dominates it lies — not only will this make the allocation scheme adaptable to a wide variety of uses, it will also be used to demonstrate correctness.

²The term *standard dominating set* is intended to agree with various definitions of dominating set used when distance is not a consideration.

Location of			
Supervertex	Index 0	Index 1	Index 2
000	CH	CH	CH
001	CR	CL	R
010	R	CR	CL
011	CL	R	CR
100	R	CR	CL
101	CL	R	CR
110	CR	CL	R
111	CH	$\overline{C}H$	$\overline{C}H$

Table 1: Marking of CCC₃ showing a Standard Perfect Dominating Set

	10	11	01
00	CH	CH	CH
01	CR	CL	R
10	R	CR	CL
11	CL	R	CR

Table 2: First Labeling Scheme Component

2.1 Vertex Marking

Each vertex in \mathbf{CCC}_k has two neighbors within the cycle and one neighbor adjacent along its hypercube edge. Thus, four possibilities exist for each vertex. Either it is a resource node (in the perfect dominating set), the vertex which covers it lies across the hypercube edge, or the vertex which cover it lies to the left or right within the cycle. Formalizing the description:

- R a member of the perfect dominating set (a *Resource* node)
- CH dominated by the adjacent vertex along the dimension indicated by the index (Covered along a Hypercube edge)
- CL dominated by the adjacent vertex within the same cycle to the left meaning the vertex whose index is 1 more (mod k) (Covered by a node to the Left)
- CR dominated by the adjacent vertex within the same cycle to the right meaning the vertex whose index is 1 less (mod k) (Covered by a node to the Right)

A solution for k = 3 (d = 1) is presented with these labels in table 1 (inspection of figure 2 suffices to verify that this is, indeed, a **PDS**₁).

2.2 The Method

The general solution for d = 1, $k \neq 5$ is generated using copies of Table 2 and Table 3. First, the value of k is decomposed into 3a + 4b where a and b are nonnegative integers (note that this is possible for all k > 3 with the exception of 5). Then, a copies of the first component (table 2) are concatenated with b copies of the second component (table 2). As an example, when k = 11, the example shown in table 4 might be produced.



Figure 2: Cube-Connected Cycle of order 3 with Perfect Dominating Set (d = 1)

	10	10	10	10
00	CH	CL	R	CR
01	CR	CH	CL	R
10	R	CR	CH	CL
11	CL	R	CR	CH

Table 3: Second Labeling Scheme Component

	10	11	01	10	10	10	10	10	10	10	10
00	CH	CH	CH	CH	CL	R	CR	CH	CL	R	CR
01	CR	CL	R	CR	CH	CL	R	CR	CH	CL	R
10	R	CR	CL	R	CR	CH	CL	R	CR	CH	CL
11	CL	R	CR	CL	R	CR	CH	CL	R	CR	CH

Table 4: Example Concatenation of Components

Now, given the position of any vertex in CCC_k , its index and the location of the supervertex within the hypercube, the composite table can be used to provide a marking for each vertex such that the vertices marked with R form a perfect dominating set.

Thus, in order to find the appropriate designation for $10\hat{1}00100000$, note that the supervertex located at 10100100000 has high bits in three locations — the first, third and sixth positions from left to right — corresponding to values 10, 01, and 10; since $10 \oplus 01 \oplus 10$ is 01, the row labelled 01 will be used; the column is that underneath the accented 1; and, hence, $10\hat{1}00100000$ will be marked as a resource node.

2.3 Correctness:

The row chosen is dependent only on the location of the supervertex. Thus, the labeling within each cycle can be read directly from the appropriate row of the table. Hence, it can quickly verified that, from left to right (and wrapping around the end), the constraints on a **PDS**₁ are followed within each supervertex — that each vertex with designation R has left and right neighbors appropriately labeled CR and CL, etc. (note that the tables above are constructed so that concatenation preserves this property). What may or may not be so quickly verified is that edges between supervertices are also properly used (a vertex is marked with CH/R if and only if it has a neighbor along its hypercube edge with designation R/CH).

Note that two supervertices connected to one another along dimension i are connected at the vertex with index i. Thus, two vertices which are connected by an edge not in a cycle (a hypercube edge) have the same index, i; the designations, therefore, come from the same column. Note also that supervertex locations must differ in exactly one bit — the bit with index i. Thus, the row used to label one vertex is different from that vertex's (only) cube-edge neighbor by an XOR operation with entry above column i. Now, a closer examination of the columns of each initial table confirms that, for any row label, bitwise XOR'ing with that binary value will not map the designation R/CH onto any designation than CH/R.

Now, since every vertex has a designation, R, CH, CL, or CR; no vertex with designation R has any neighbor marked incorrectly, and each of the markings CH, CL, and CR correctly indicate the presence of a resource node, it follows that the process of marking indicated by the tables has, in fact, generated a perfect dominating set.

2.4 A Proof of the Non-existence of a PDS_1 for k = 5

It does not follow that no **PDS**₁ exists when k = 5 simply because the above generating scheme does not produce a proper marking for that case. The argument for nonexistence is more subtle. There are 5×2^5 (160) vertices in **CCC**₅. If a **PDS**₁ did exist, since each vertex covers exactly four neighbors, it would contain exactly $5 \times 2^{5-2}$ (40) elements. By inspection, no supervertex can contain more than one element from the **PDS**₁. Since there 2^5 (32) supervertices, by the pigeon-hole principle, some supervertex must contain more than one element. Hence, the assumption that a **PDS**₁ did exist is contradicted.

3 Nonexistence of Perfect Dominating Sets with Greater Distances

With the exception of the distance equaling or exceeding the diameter of \mathbf{CCC}_k , when no \mathbf{PDS}_d for \mathbf{CCC}_k exists when d > 2. This can be restated as no \mathbf{PDS}_d with more than one vertex exists for \mathbf{CCC}_k when d > 2. (Note: If d is less than the diameter of \mathbf{CCC}_k , more than one vertex is necessary — this is not true for all graphs, but follows from the automorphisms of \mathbf{CCC}_k .)

The argument for nonexistence proceeds as follows: When $d \ge 5$, the pattern of vertices covered by a single vertex is sufficiently "irregular" to preclude the construction of a \mathbf{PDS}_d with more than one element. For $2 \le d \le 4$, examination of various conditions on the number of vertices covered by a single vertex will handle the majority of the remaining cases.

3.1 Elimination of Large Values of d

The first set of cases will be all but a finite number of values for d. Specifically, the existence of a PDS_d with more than element is shown not to be possible when $d \ge 5$.

The general technique is to choose an arbitrary vertex v_0 from \mathbf{CCC}_k , and demonstrate that there exists a vertex v which is *isolated* — it is not covered by v_0 and any vertex which does cover it also covers some vertex which is already covered by v_0 . Thus, if we start to construct a perfect dominating set by the inclusion of v_0 , we cannot include a vertex which covers v without having some vertex covered twice.

(By the symmetries of \mathbf{CCC}_k , any arbitrary vertex is isomorphic to a particular vertex; so, it is sufficient to demonstrate an isolated vertex v when v_0 is $\hat{0}0^{k-1}$. This vertex will be referred to as the zero of \mathbf{CCC}_k .)

3.1.1 Useful Definitions and Lemmas

Lemma 3.1.1 Any path in CCC_k with the locations of the supervertices containing the endpoints differing in bit position p must include a visit to a vertex with index p.

PROOF: The set of hypercube edges along dimension i form a cutset; thus, the described path must include one of these edges. The lemma follows immediately from the fact that the only vertices incident to these edges have index i.

Lemma 3.1.2 (The Distance Calculation Lemma) Let v_0 and v_1 be vertices in CCC_k such that v_0 has index i_0 , v_1 has index i_1 , and the locations of the supervertices containing v_0 and v_1 differ in the bit positions described by the set $H = \{p_0, \ldots, p_{h-1}\}$. If x be the number of edges in the shortest walk on the k-cycle starting at index i_0 and ending at index i_1 which includes a visit to every vertex with an index in the set H then x + h is the distance in CCC_k from a vertex v_0 to a vertex v_1 .

PROOF: Without loss of generality, let v_0 be vertex i_0 at the origin in CCC_k , and let v_1 be vertex i_1 in the supervertex whose location has high bits in positions described by H. Any path from v_0 to v_1 must include at least h hypercube edges. Removing these edges from the path and mapping the remaining cycle-edges onto the k-cycle in obvious manner will form a walk on the k-cycle. This walk starts at vertex i_0 , ends at vertex i_1 , and visits every vertex with an index in the set H. The length of this walk must be at least x. So the distance from v_0 to v_1 is least x + h.

Now, given a walk W in the k-cycle from vertex i_0 to vertex i_1 which visits every vertex with an index in the set H which has length x, we can construct a walk from v_0 to v_1 in the following way: Starting at v_0 , if the

current vertex is the first vertex encountered with an index in H, include the hypercube edge and proceed; otherwise take the next edge in W, map it onto the current supervertex, and proceed along that edge. This walk has length x + h, so the distance from v_0 to v_1 must be at most x + h, and the lemma follows.

Corollary 3.1.1 Let v_0, v_1, v_2 be vertices in CCC_k . The distance from v_0 to v_1 is less than the distance from v_0 to v_2 if the index of v_1 is equal that of v_2 and set of bit positions where the supervertices containing v_0 and v_1 differ is a proper subset of the set of bit positions where the supervertices containing v_0 and v_2 differ.

Lemma 3.1.3 The diameter (the greatest distance between any two vertices in a specified graph) of CCC_k is $\lfloor \frac{5k}{2} - 2 \rfloor$ when k > 3; when k = 3, the diameter is 6.

PROOF: Let v_0 be the zero of \mathbf{CCC}_k (equivalent to an arbitrary choice). Now, by the above corollary, if v_1 is any vertex in \mathbf{CCC}_k with index i_1 , then the distance from v_0 to v_1 is *not* greater than the distance from v_0 to the vertex with index i_1 in the supervertex whose location has only high bits. Thus, it is sufficient to find the index i_1 such that the shortest walk from 0 to i_1 on the k-cycle which visits *all* vertices is maximal. By inspection, $i_1 = 0$ suffices for the case k = 3 and $i_1 = \lfloor \frac{k}{2} \rfloor$ suffices for all other cases.

Lemma 3.1.4 $k > \frac{4d}{5}$ is a necessary condition for the existence of a PDS_d with more than one vertex for CCC_k.

PROOF: If a **PDS**_d with more than one element exists for **CCC**_k, then the shortest path between any two elements in that **PDS**_d is at least 2d + 1. Because that distance is at most the diameter of **CCC**_k, when $k \ge 4$, $2d + 1 \le \lfloor \frac{5k}{2} - 2 \rfloor$, and immediately $d < \frac{5k}{4}$. When k = 3, the diameter is 6, and the maximum allowable distance for a **PDS**_d is 2; thus, the lemma follows.

3.1.2 Isolated Points for Certain Values of d

Let d = 8, and, therefore, k > 6, and the vertices

$$v = 1010^{(k-4)} 1$$

$$n_1 = 1010^{(k-4)} 1$$

$$n_2 = 0010^{(k-4)} 1$$

$$n_3 = 1010^{(k-4)} 1$$

are well-defined.

Now, v is not covered by (within distance d of) the zero of \mathbf{CCC}_k . This is the first application of the distance calculation lemma; so, explicitly: the shortest walk on the k-cycle from 0 to 0 which visits vertices in $\{0, 1, 2, k - 1\}$ has length 6 (by inspection — recall that k is least 6, making a cycle tour at least as long as the walk given by the vertex sequence (0, 1, 2, 1, 0, k - 1, 0)); thus, the distance from the zero of \mathbf{CCC}_k to v is 6 + 3 (the number of hypercube edges traversed and/or the number of high bits in the location of the supervertex containing v).

However, all of the neighbors of v (exactly n_1 , n_2 , and n_3) are covered by the zero of \mathbf{CCC}_k (this also follows from the distance calculation lemma). Since any vertex which covers v must also cover at least one of its neighbors, the vertex v is isolated. (In fact, this is a stronger condition – for every vertex v_1 such that $d(v, v_1) = d$, any path of length d connecting v_1 and v must *include* a vertex which is covered by the zero.)

Thus, it is not possible, when d = 8, to select a set of vertices which cover all vertices in CCC_k without some vertex being covered at least twice. Hence, when d = 8, no PDS_d exists for CCC_k .

Similarly, when d = 10 and $v = \hat{1}010^{(k-6)}10$, or d = 13 and $v = \hat{1}0110^{(k-7)}10$, v can be shown to be isolated. In both cases, the zero of **CCC**_k does not cover v, but does cover all three neighbors of v.

Not every value of d where $d \ge 5$ will produce a vertex which is not covered by the zero, but has all three neighbors covered by the zero. However, it will be possible to demonstrate a vertex v which is not covered by the zero and a set \mathcal{B} of vertices which are covered by the zero so that every vertex which covers v must cover some vertex in \mathcal{B} .

For d = 5, let $v = \hat{0}10^{(k-3)1}$ and let \mathcal{B} be the set $\{b_0, b_1, b_2, b_3\}$ where $b_0 = 1\hat{0}0^{(k-3)}1$, $b_1 = 110^{(k-3)}\hat{0}$, $b_2 = 0\hat{1}0^{(k-3)}1$, and $b_3 = 010^{(k-3)}\hat{1}$. Every vertex in \mathcal{B} is covered by the zero, v is not, and all vertices in $\mathcal{B} \cup \{v\}$ are well defined.

Let v_1 be any vertex which covers v. If $d(v, v_1) < 5$, v_1 must cover b_2 and b_3 as well as v. Otherwise, $d(v, v_1) = 5$ and, if v_1 does not cover either b_2 and b_3 , $d(\hat{1}10^{(k-3)}1, v_1) = 4$. Moreover, either $d(\hat{1}10^{(k-3)}1, v_1) = 3$ or $d(110^{(k-3)}\hat{1}, v_1) = 3$. Assume that $d(110^{(k-3)}\hat{1}, v_1) = 3$; since $d(110^{(k-3)}\hat{1}, b_1) = 1$, $d(b_1, v_1) = 4$. Otherwise, $d(\hat{1}10^{(k-3)}1, v_1) = 3$; since $d(\hat{1}10^{(k-3)}1, b_0) = 1$, $d(B_1, v_1) = 4$. Thus, any vertex which covers v must cover some vertex in \mathcal{B} and v is isolated.

A similar argument suffices for the case d = 7 with

$$v = \hat{0}010^{(k-4)}1$$
 and $\mathcal{B} = \left\{00\hat{1}0^{(k-4)}1, \ 00\hat{0}0^{(k-4)}1, \ 0010^{(k-4)}\hat{1}, \ 0010^{(k-4)}\hat{0}
ight\}$

Thus, when $d \in \{5, 7, 8, 10, 13\}$, an isolated vertex exists, and it is not possible to construct a **PDS**_d for **CCC**_k.

3.1.3 Isolated Points for Large Values of d

Let d = 3n+2m+i where n, m, and i are integer values such that $n \ge m \ge i > 0$. Note that appropriate values for n, m, and i can be chosen to produce any positive integer except those in $\{1, 2, 3, 4, 5, 7, 8, 10, 13\}$. Let v denote $\hat{1}1^{(n)}0^{(k-m-n-1)}1^{(m)}$. Since

$$k > \frac{4(3n+2m+i)}{5}$$

>
$$2n+m+\frac{m+i}{5}$$

>
$$2n+m+i$$

>
$$n+m+1$$

this v is well-defined.

Now, the length of the shortest walk on the k-cycle from 0 to 0 which visits all vertices in

 $H = \{m - k, m - k + 1, \dots, k - 1, 0, 1, \dots, n\}$ is the minimum of k (corresponding to a complete cycle tour) and 2n + 2m (any other walk must visit both n and k - m and, since it is closed, each edge will be included twice). Since k > 2n + m + i and $m \ge i$ implies that $2n + 2m \ge 2n + m + i$, 2n + m = i is a lower bound on the length of that walk. Thus, by the distance calculation lemma, the distance from the zero of \mathbf{CC}_k to v is at least (2n + m + i) + (n + m + 1), which is greater than d. Thus, v is not covered the zero of \mathbf{CCC}_k .

Let \mathcal{B}_n be the set

$$\left\{B_0B_1\dots B_{n-1}\hat{B_n}0^{(k-m-n-1)}B_{k-m}\dots B_{k-1}: \forall j \in H, B_j \in \{0,1\}\right\}$$

and let \mathcal{B}_m be the set

$$\left\{B_0 B_1 \dots B_n 0^{(k-m-n-1)} \hat{B_{k-m}} B_{n-k+1} \dots B_{k-1} : \forall j \in H, B_j \in \{0,1\}\right\}$$

and let $\mathcal{B} = \mathcal{B}_n \bigcup \mathcal{B}_m$.

Both $1^{(n)} \hat{1} 0^{(k-m-n-1)} 1^{(m)}$ and $1^{(n+1)} 0^{(k-m-n-1)} \hat{1} 1^{(m-1)}$ are covered by the zero of \mathbf{CCC}_k (the length of the shortest walk from 0 to n in the k-cycle which includes vertices from H is at most n + 2m; the length of the shortest walk from 0 to k - m in the k-cycle which includes vertices from H is at most 2n + m; $(n+2m) + (n+m+1) \leq (2n+m) + (n+m+1) \leq d$). Thus, by the corollary to the distance calculation lemma, it follows that every element of \mathcal{B} is also covered by the zero of \mathbf{CCC}_k .

Let v_1 be any vertex in \mathbf{CCC}_k within d distance of v. Let i_1 denote the cycle index of v_1 , and let H_1 be the set of bit positions where supervertices containing v and v_1 differ. Now, choose a vertex b_n from \mathcal{B}_n and a vertex b_m from \mathcal{B}_m such that $\forall j \in H$, the *j*th bit of the location of the supervertex containing b_n and b_m agrees with the corresponding bit of the supervertex containing v_1 .

If $H_1 \sim H$ (the set of indices from H_1 which do not appear in H) is empty, both b_n and b_m lie in the same supervertex as v_1 and, immediately, at least one of b_n and b_m is within distance d of v_1 (v_1 is within distance d of the vertex with cycle index 0). Otherwise, the shortest walk on the k-cycle from i_1 to 0 which visits all vertices from $H_1 \sim H$ ends with a path from either n or k - m to 0. Thus, there is a walk on the k-cycle starting at i_1 , visiting every vertex in $H_1 \sim H$, and ending at either n or k - mwhich is shorter. Since $H_1 \sim H \subseteq H_1$, one of either b_n or b_m is closer to v_1 than v. Since any vertex which covers v also covers some vertex already covered by the zero of \mathbf{CCC}_k , if d is any value not in $\{1, 2, 3, 4, 5, 7, 8, 10, 13\} \sim \{5, 7, 8, 10, 13\}$, no \mathbf{PDS}_d exists containing more than one element for \mathbf{CCC}_k . COMMENT: When d < 5, it is possible to show that no isolated vertices exist.

3.2 Nonexistence of Perfect Dominating Sets for $2 \le d \le 4$

Let C(d, k) be the number of vertices in \mathbf{CCC}_k covered by a single vertex. By the isomorphic properties of \mathbf{CCC}_k , C(d, k) is a constant for fixed k and d. In fact, it will be shown that when k > 2d, C(d, k) depends only on the value of d.

For most of the remaining cases, when $2 \le d \le 4$, C(d, k) will shown later to contain an odd prime factor p which either does not divide k or is greater than 2d. Both conditions preclude the existence of a **PDS**_d for **CCC**_k. The first is shown immediately with the following lemma:

Lemma 3.2.1 If there exists a PDS_d for CCC_k and C(d, k) contains an odd prime factor p, then k is divisible by p.

PROOF: There are $k \times 2^k$ vertices in **CCC**_k. Each element in the **PDS**_d must cover exactly C(d, k) vertices; so, $\frac{k2^k}{C(d,k)}$ (the number of vertices in a **PDS**_d) is an integer, and the lemma follows.

The structure of the argument for the second will be to show that a necessary condition for the existence of a \mathbf{PDS}_d for \mathbf{CCC}_k when k is a multiple of exactly n factors of an odd prime p such that p > 2d is that the number of elements in the \mathbf{PDS}_d must be divisible by p^n (this is trivially true when n = 0). Therefore, for any prime p > 2d, given that k contains exactly n factors of p, $\frac{k}{p^n} \frac{2^k}{C(d,k)}$ must be an integer — implying immediately that C(d, k) cannot contain any prime factor greater than 2d. Hence, if C(d, k) does contain a prime factor p greater than 2d, no \mathbf{PDS}_d exists for \mathbf{CCC}_k .

3.2.1 Necessary Definitions

By the automorphisms of \mathbf{CCC}_k , if some vertex with index *i* covers exactly *n* vertices with index *j*, then every vertex with index *i* covers exactly *n* vertices with index *j*. The following definitions make that property explicit and offer a straightforward method of calculating the value of *n*.

Definition 3.2.1 Let $C(d, k)_j$ be the number of distinct subsets H of $\{0, \ldots, k-1\}$ such that there exists a walk of length x on the k-cycle which starts at index d, visits all vertices in H, and ends at index j subject to $x + |H| \leq d$.

Lemma 3.2.2 $C(d, k)_j$ is the number of distinct vertices with index j in CCC_k which are within d distance of a single vertex with an index d.

PROOF: This follows from the distance calculation lemma. With H taken as a set of bit positions, each distinct subset of H uniquely describes a supervertex location within \mathbf{CCC}_k and, together with j, a unique vertex in \mathbf{CCC}_k .

Corollary 3.2.1 The number of vertices covered by a single vertex, C(d, k), is

$$\sum_{i=0}^{k-1} C(d,k)_i$$

Corollary 3.2.2 For all $i, j \in \{0, ..., k-1\}$, the number of distinct vertices with index i which can be covered by a single vertex with index j is $C(d, k)_{(d+i-j \mod k)}$.

CLARIFICATION: This follows from the automorphisms of \mathbf{CCC}_k . If a vertex with index j covers c vertices with index i, then a vertex with index $(j + x \mod k)$ covers c vertices with index $(i + x \mod k)$. It now follows that, for large values of k, C(d, k) does not depend on k. Since our concern is now with a finite set of values of d, the set of values of C(d, k) and $C(d, k)_j$ under consideration will also be finite (and calculable by the method implicit in the definition of $C(d, k)_j$).

Lemma 3.2.3 For all k > 2d, $C(d, k)_j = C(d, 2d + 1)_j$.

PROOF: When k > 2d, the value of $C(d, k)_j$ does not depend on k. No walk of length at most d starting at d visits any vertex outside of the set $S = \{0, 1, ..., 2d - 1, 2d\}$. Immediately, any $H \not\subseteq S$ need not be considered and $\forall j \notin S$, $C(d, k)_j = 0$.

Corollary 3.2.3 For all k > 2d, C(d, k) = C(d, 2d + 1).

Corollary 3.2.4 For all j > 2d, $C(d, 2d + 1)_j = 0$.

Now, given that a single vertex with index j covers exactly $C(d, k)_{(d+i-j \mod k)}$ vertices with index i, if X_j is the number of elements in a **PDS**_d for **CCC**_k with index j, then the sum over j of $X_jC(d, k)_{(d+i-j \mod k)}$ is total number of vertices in **CCC**_k with index i. This property and similar necessary conditions can be expressed as matrix relationships. The following definition will be useful in that regard.

	0	10	10	1.1	c	1	0	0	0	0	0	0	0	0	0	0	1	e	1.1	10	10 .
1		10	10	11	0	1	0	0	0	0	0	0	0	0	0	0	1	0	11	10	10
1	10	8	10	10	11	6	1	0	0	0	0	0	0	0	0	0	0	1	6	11	10
	10	10	8	10	10	11	6	1	0	0	0	0	0	0	0	0	0	0	1	6	11
	11	10	10	8	10	10	11	6	1	0	0	0	0	0	0	0	0	0	0	1	6
	6	11	10	10	8	10	10	11	6	1	0	0	0	0	0	0	0	0	0	0	1
	1	6	11	10	10	8	10	10	11	6	1	0	0	0	0	0	0	0	0	0	0
	0	1	6	11	10	10	8	10	10	11	6	1	0	0	0	0	0	0	0	0	0
	0	0	1	6	11	10	10	8	10	10	11	6	1	0	0	0	0	0	0	0	0
	0	0	0	1	6	11	10	10	8	10	10	11	6	1	0	0	0	0	0	0	0
	0	0	0	0	1	6	11	10	10	8	10	10	11	6	1	0	0	0	0	0	0
	0	0	0	0	0	1	6	11	10	10	8	10	10	11	6	1	0	0	0	0	0
	0	0	0	0	0	0	1	6	11	10	10	8	10	10	11	6	1	0	0	0	0
	0	0	0	0	0	0	0	1	6	11	10	10	8	10	10	11	6	1	0	0	0
	0	0	0	0	0	0	0	0	1	6	11	10	10	8	10	10	11	6	1	0	0
	0	0	0	0	0	0	0	0	0	1	6	11	10	10	8	10	10	11	6	1	0
	0	0	0	0	0	0	0	0	0	0	1	6	11	10	10	8	10	10	11	6	1
	1	0	0	0	0	0	0	0	0	0	0	1	6	11	10	10	8	10	10	11	6
	6	1	0	0	0	0	0	0	0	0	0	0	1	6	11	10	10	8	10	10	11
	11	6	1	0	0	0	0	0	0	0	0	0	0	1	6	11	10	10	8	10	10
1	10	11	6	1	0	0	0	0	0	0	0	0	0	0	1	6	11	10	10	8	10
/	10	10	11	6	1	0	0	0	0	0	0	0	0	0	0	1	6	11	10	10	8 /

Figure 3: Example: M(5, 21)

Definition 3.2.2 For all $n \geq 2d + 1$, let M(d, n) denote the $n \times n$ matrix such that $M(d, n)_{i,j} = C(d, 2d + 1)_{(d+i-j \mod n)}$.

An example of such a matrix is shown in figure 3.

3.2.2 Properties of $M(d, p^n)$

Examining the definition, we find that $M(d, n)_{i,j} = M(d, n)_{(i+1 \mod n), (j+1 \mod n)}$. In essence, each row of M(d, n) is the previous row "shifted" right (with wrap-around). Other properties of interest are:

Lemma 3.2.4 Each row R in M(d, n) is nonzero, has no negative entries, and, in fact, has at least two distinct nonzero entries.

PROOF: Applying the calculation method implicit in the definition of C(d, 2d + 1), C(d, 0) = 1 and C(d, 1) = d + 1. Let R be the *j*th row of M(d, n), and, WLOG, assume $j \ge d$, the (j - d)th entry in R, $M(d, n)_{(j-d), j}$, is 1 and the (j - d + 1)th entry in R is d + 1.

Lemma 3.2.5 When n = qp where p > 2d, each row R in M(d, n) has the property that for all j, the *i*th entry in R is nonzero for at most one value of $i \equiv j \pmod{p}$.

PROOF: Recalling that $C(d, 2d + 1)_j = 0$ for all $j \ge 2d + 1$, then $C(d, 2d + 1)_{(d+i-j \mod n)}$ nonzero implies that $d+i-j \mod n$ is less than 2d+1 and, therefore, less than p. If $i_0 \equiv i_1 \pmod{p}$, but $i_0 \not\equiv i_1 \pmod{p}$, then at most one of $d+i_0-j \mod pq$ and $d+i_1-j \mod pq$ is less than p. By the definition, at most one of $M(d, n)_{i_0,j}$ and $M(d, n)_{i_1,j}$ is nonzero.

Lemma 3.2.6 M(d, n) has rank at least n - 2d.

PROOF: By inspection, the rows d through n - d - 1 are in diagonal form. (When $j \in \{d, d + 1, ..., n - d - 1\}$ and i < j - d, d + i - j is an element of $\{2d + 1 - n, 2d + 2 - n, ..., -1\}$. Since $n \ge 2d + 1$, $(d + i - j \mod n) \ge 2d + 1$ and $M(d, n)_{i,j} = 0$.)

Theorem 3.2.1 Let n be a positive integer, $M(d, p^n)$ is regular when p > 2d and p is prime.

PROOF: Let L be the isomorphism from $\Re^{(p^n)}$ to itself which sends the *i*th standard basis vector ³ to the $(i + 1 \mod p^n)$ th standard basis vector.

Treating L purely as a linear transformation, the minimum polynomial of L is $\mu(\lambda) = \lambda^{(p^n)} - 1$. (The minimum polynomial of a linear transformation L is the nonzero polynomial μ of least degree such that $\forall v, (\mu(L))(v) = 0$ ⁴.) Verification is immediate since both $L^{(p^n)}$ and $I_p^{(0)}$ are the identity transformation, thus

$$\forall v \in \Re^p, (\mu(I_p))(v) = (I_p^{(p)} - I_p^{(0)})(v) = I_p^{(p)}(v) - I_p^{(0)}(v) = 0$$

Minimality follows from consideration of the operation of any nonzero polynomial of degree less than p^n on a standard basis vector.

Now, for any nonzero vector v, the order of v with respect to a linear transformation L is the nonzero polynomial μ_v of least degree such that $(\mu_v(L))(v) = 0$. The minimum polynomial μ is a multiple of the order of any vector; thus, for any nonzero vector $v \in \Re^{(p^n)}$, the only possible values for μ_v are factors of $\lambda^{(p^n)} - 1$. As shown in appendix 3.4, a complete factorization of $\lambda^{(p^n)} - 1$ is

$$\{\lambda - 1\} \bigcup \left\{ \sum_{i=0}^{p-1} \lambda^{(ip^j)} : j \in \{0, 1, \dots, n-1\} \right\}.$$

Define S(v) as the subspace spanned by $\{L^{(n)}(v) : n > 0\}$. (Formally, S(v) is an invariant subspace of $\Re^{(p^n)}$, the cyclic space relative to L generated by the vector v.) The degree of the order of v is the rank of the subspace S(v). (Let μ_v have degree r, $\mu_v(L)(v) = 0$ implies that $L^{(r)}(v)$ is a linear combination of vectors from

$$\left\{ L^{(n)}(v) : 0 \le n \le r - 1 \right\}.$$

Since $\mu_v(L)(v)$ has minimal degree, there does not exist $r_0 \leq r$ such that $L^{r_0}(v)$ is a linear combination of vectors from $\{L^{(n)}(v): 0 \leq n \leq r_0 - 1\}$. Thus, S(v) has

$$\left\{I_p^{(n)}(v): 0 \le n \le r-1, \text{ where } r \text{ is the degree of } \mu_v\right\}$$

as a basis, and, directly, the rank of S(v) is the number of vectors in that basis, r.)

Now consider the order of R, an arbitrary row of $M(d, p^n)$. S(R) is, by definition, the subspace of $\Re^{(p^n)}$ spanned by the row vectors of $M(d, p^n)$ ($L^{(i)}(R)$ is also a row in $M(d, p^n)$) for arbitrary i; and for any row R' in $M(d, p^n)$, there exists an i such that $R' = L^{(i)}(R)$). Thus, degree of μ_R is the rank of $M(d, p^n)$.

Since *R* is nonzero and has no negative entries; $(\lambda^{p^n-1} + \lambda^{p^n-2} + \dots + \lambda + 1)(L)(R)$ is a nonzero vector and μ_R is not a factor of $\lambda^{p^n-1} + \lambda^{p^n-2} + \dots + \lambda + 1$. Thus, μ_R must be a multiple of $(\lambda - 1)$.

Recall that R has two distinct nonzero entries and that for all j, the *i*th entry in R is nonzero for at most one value of $i \equiv j \pmod{p}$. Thus,

$$R' = \left(\sum_{i=0}^{p^{(n-1)}-1} \lambda^{(ip)}\right) (L)(R)$$

³The *n*th standard basis vector for \Re^m is the unique vector $\vec{V} \in \Re^m$ with the *n*th entry, the only nonzero entry, equal to 1. As used here, the enumeration of positions begins with 0; thus, the 0th standard basis vector denotes (1, 0, ...).

⁴The definition often includes the restriction that the leading coefficient must be 1 to avoid ambiguity.

is a nonzero vector with at least two distinct entries. Immediately, $(\lambda - 1)(L)$ applied to that vector is nonzero. Since

$$\begin{aligned} ((\lambda - 1)(L))(R') &= ((\lambda - 1)(L)) \left(\left(\sum_{i=0}^{p^{(n-1)}-1} \lambda^{(ip)} \right)(L) \right) \right)(R) \\ &= \left((\lambda - 1) \left(\sum_{i=0}^{p^{(n-1)}-1} \lambda^{(ip)} \right) \right)(L)(R) \\ &= \left(\frac{\lambda^{(p^n)} - 1}{\sum_{i=0}^{p-1} \lambda^i} \right)(L)(R) \end{aligned}$$

is a nonzero vector, μ_R has $(\sum_{i=0}^{p-1} \lambda^i)$ as a factor.

Since the rank of $M(d, p^n)$ is at least $p^n - 2d$, μ_R cannot be a factor of

$$\frac{\lambda^{(p^n)} - 1}{\sum_{i=0}^{p-1} \lambda^{(ip^j)}}$$

for $j \ge 1$ since, otherwise, the degree of μ_R would be $p^n - (p-1)p^j$ which, when $j \ge 1$ is less than $p^n - 2d$. Thus, μ_R must include $(\sum_{i=0}^{p-1} \lambda^{(ip^j)})$ as a factor for all $j \ge 0$.

It follows that the order of R must be $\lambda^{(p^n)} - 1$. The degree of μ_R being p^n , the rank of $M(d, p^n)$ is therefore p^n and, since $M(d, p^n)$ is a $p^n \times p^n$ matrix, $M(d, p^n)$ is regular (invertible).

3.2.3 The Relation of M(d, k) to a PDS_d for CCC_k

Now the regularity of $M(d, p^n)$ is applied to show the following theorem:

Theorem 3.2.2 Let $k = qp^n$ where p is an odd prime such that p > 2d, and n and q are positive integers. If there exists a PDS_d for CCC_k , then the number of elements in the PDS_d must be divisible by p^n .

PROOF: Let k, p, n, and q be as described, and define the p^n -index of a vertex as its cycle index mod p^n (this notation is purely for convenience of expression). Now, the proof can be expressed in the following two lemmas.

Lemma 3.2.7 $M(d, p^n)_{i,j}$ is the number of distinct vertices in CCC_k with p^n -index j which can covered by a single vertex with p^n -index i

PROOF: By an earlier lemma, the number of distinct vertices with index j which can be covered by a single vertex with index i is $C(d, k)_{(d+i-j \mod p^n)}$; therefore, for $j \in \{0, \ldots, p^n - 1\}$, the number of vertices with an index equivalent to j modulo p^n which can be covered by a single vertex with index i (WLOG, p^n -index i) is $\sum_{\ell=0}^{q-1} C(d, k)_{(d+i+\ell p^n - j \mod k)}$. Now, $C(d, k)_{(d+i+\ell p^n - j \mod k)}$ is zero when $d + i + \ell p^n - j \mod 2 2 d + 1$, implying that, $C(d, k)_{(d+i+\ell p^n - j \mod k)}$ is nonzero for at most value of ℓ . In fact, $\sum_{\ell=0}^{q-1} C(d, k)_{(d+i+\ell p^n - j \mod k)} = C(d, k)_{(d+i-j \mod p^n)}$. Because $M(d, p^n)_{i,j} = C(d, 2d + 1)_{(d+i-j \mod p^n)} = C(d, k)_{(d+i-j \mod p^n)}$, the lemma follows.

Definition 3.2.3 Let X be any set of vertices from CCC_k and let \vec{X} denote the column vector in \Re^k whose *i*th entry, \vec{X}_i , is the number of elements in X with p^n -index i.

Lemma 3.2.8 If X is a PDS_d, then $M(d, k) \times \vec{X} = (2^k q \ 2^k q \ \cdots \ 2^k q)^T$.

PROOF: If X is a \mathbf{PDS}_d , then every vertex in \mathbf{CCC}_k with p^n -index j must be covered by exactly one vertex from X. The number of distinct vertices with p^n -index j covered by a single vertex with p^n -index i is $M(d, k)_{i,j}$; the number of elements in X with p^n -index i is \vec{X}_i . No vertex in \mathbf{CCC}_k is covered by more one element of X; so, $M(d, k)_{i,j}$ multiplied by \vec{X}_i . must be the total number of distinct vertices with p^n -index i covered by the vertices in X with p^n -index j. It follows that if R_j is the jth row of $M(d, p^n)$, then $R_j \vec{X}$ must be the total number of distinct vertices with p^n -index j covered by the set X. Since X is a \mathbf{PDS}_d , this be must the total number of vertices in \mathbf{CCC}_k with p^n -index j. The lemma then follows from the definition of matrix multiplication and the fact that there are exactly 2^k vertices in \mathbf{CCC}_k with any arbitrary index i — and, thus, $2^k q$ vertices with any arbitrary p^n -index i.

Since $M(d, p^n)$ is regular, any p^n length column vector \vec{Y} such that $M(d, k) \times \vec{Y} = (2^k q \ 2^k q \ \cdots \ 2^k q)^T$ must have uniform entries. (One solution for \vec{X} is

$$\left(\frac{2^k q}{\sum_{i=0}^{p^n-1} M(d,p^n)_{i,j}} \frac{2^k q}{\sum_{i=0}^{p^n-1} M(d,p^n)_{i,j}} \cdots \frac{2^k q}{\sum_{i=0}^{p^n-1} M(d,p^n)_{i,j}}\right)^{\mathbf{T}}$$

Immediately, since $M(2d, p^n)$ is invertible, this is the *only* solution.) Noting that the entries in \vec{X} must be integers, it follows that the sum of the entries in \vec{X} must be an integer which is divisible by p^n . Under the assumptions stated earlier, the number of vertices in X, an arbitrary PDS_d for CCC_k , is the sum of the entries in \vec{X} ; thus, the number of elements in an arbitrary PDS_d for CCC_k must be divisible by p^n .

Theorem 3.2.3 If C(d, k) has any prime factor p > 2d, no PDS_d exists for CCC_k .

PROOF: Recall that the number of elements in any \mathbf{PDS}_d for \mathbf{CCC}_k must be $\frac{k2^k}{C(d,k)}$, an integer. For any prime p > 2d, k can be written as $= qp^n$ where n is a nonnegative integer and q a positive integer not divisible by p. By the above, for any \mathbf{PDS}_d for \mathbf{CCC}_k , for any prime p > 2d, $\frac{q2^k}{C(d,k)}$ must be an integer for some value of q not divisible by p.

3.2.4 Specific Cases

Now, listing the calculated values of C(d, k) in Table 5 (and noting that for k > 2d, C(d, k) = C(d, 2d+1)), there are exactly two cases where C(d, k) does not either contain a prime p > 2d or any prime p where k is not divisible by p — when d = 2 and k = 3 and when d = 3 and k = 5. This are small graphs, and an exhaustive search reveals that, in these cases as well, there does not exist a **PDS**_d for **CCC**_k. Hence, for all d > 1, no **PDS**_d exists for **CCC**_k.

COMMENT: When d = 5, C(d, 2d + 1) is 84. While a similar matrix argument exists, the one given here does not suffice. Also, it is not clear whether or the matrix argument could be generalized to handle arbitrary values of d. Thus, both arguments seem necessary.

3.3 Other Points of Interest:

There may be some extended results which limit the number of ways in which a **PDS**₁ may be constructed for $CCC_k (k \neq 5)$. Essentially, the obvious rotations, reflections, and alternate choices for a and b (such

	<i>d</i> = 2	<i>d</i> = 3	<i>d</i> = 4
<i>k</i> = 3	8	14	20
<i>k</i> = 4	9	17	28
<i>k</i> = 5	10	20	36
<i>k</i> = 6	10	21	39
<i>k</i> = 7		22	42
<i>k</i> = 8			43
<i>k</i> = 9			44

Table 5: Calculated values of C(d, k)

that $k = 3 \times a + 4 \times b$) using the above scheme might be shown to form all possible perfect dominating sets for d = 1 and certain values of k. No immediate application of this result is known to the authors.

The existence and patterns generated by isolated points may have some application to the problem of finding generalized dominating numbers – the size of the minimal set of vertices which dominates the graph with distance d.

Also, the matrix argument may be generalized to include other graphs, and has some application to the problem of dominating numbers. Work is currently in progress on Tori and related graphs.

3.4 Summary

Standard perfect dominating sets exist and be easily constructed for cube-connected cycles of any order other than 5. However, for greater distances, no perfect dominating sets with more than one element exist for any cube-connected cycle. In fact, for d > 4, an isolated vertex exists, indicating that the size of a minimal dominating set will be much larger than optimal. (For $1 < d \le 4$, a corresponding argument cannot be easily constructed.)

Appendix A Complete Factorization of $\lambda^{(p^n)} - 1$

Since

$$\lambda^{(p^n)} = (\lambda - 1) (\prod_{j=0}^{n-1} (\sum_{i=0}^{p-1} \lambda^{(ip^j)}))$$

it will be sufficient to show that each element in

$$\{\lambda - 1\} \bigcup \left\{ \sum_{i=0}^{p-1} \lambda^{(ip^j)} : j \in \{0, 1, \dots, n-1\} \right\}$$

is irreducible in order to obtain a complete factorization. The following lemma will be useful for that purpose:

Lemma .0.1 For all integers m, n, i, j and prime p,

$$\left(egin{array}{c} m \ n \end{array}
ight) \equiv \sum\limits_{\ell=0}^{i} \left(egin{array}{c} i \ \ell \end{array}
ight) \left(egin{array}{c} m-ip^{j} \ n-\ell p^{j} \end{array}
ight) \pmod{p},$$

PROOF: By induction on *j*. Noting that

$$\left(\begin{array}{c}m\\n\end{array}\right) = \sum_{\ell=0} \left(\begin{array}{c}i\\\ell\end{array}\right) \left(\begin{array}{c}m-i\\n-\ell\end{array}\right)$$

is an identity, assume that

$$\binom{m}{n} \equiv \sum_{\ell=0}^{i} \binom{i}{\ell} \binom{m-ip^{j-1}}{n-\ell p^{j-1}} \pmod{p}$$

for all m, n, i and prime p. Then, since $\begin{pmatrix} p \\ i \end{pmatrix} \equiv 0 \pmod{p}$ when i is not divisible by p,

$$\binom{m}{n} \equiv \sum_{\ell=0}^{p} \binom{p}{\ell} \binom{m-p^{j}}{n-\ell p^{j-1}} \equiv \binom{m-p^{j}}{n} + \binom{m-p^{j}}{n-p^{j}} \pmod{p}.$$

Now, by repeated application of

$$\left(\begin{array}{c}m\\n\end{array}\right) \equiv \left(\begin{array}{c}m-p^{j}\\n\end{array}\right) + \left(\begin{array}{c}m-p^{j}\\n-p^{j}\end{array}\right) \pmod{p},$$

the lemma follows.

Lemma .0.2 For all nonnegative integers j, $\sum_{i=0}^{p-1} \lambda^{(ip^j)}$ is irreducible when p is prime.

PROOF: This is a straightforward application of the Eisenstein irreducibility criteria. Let $x = \lambda - 1$ and substitute. Immediately, the resulting polynomial is monic and has constant term p. All that is now required to show that it is irreducible is show that all the other coefficients are divisible by p. The *n*th coefficient is $\sum_{i=0}^{p-1} \binom{ip^j}{n}$. Using the above identity, $\binom{ip^j}{n} \equiv \sum_{\ell=0}^{i} \binom{i}{\ell} \binom{0}{n-\ell p^j}$ which is nonzero only when $n = \ell p^j$ for some ℓ . When $n = \ell p^j$, $\binom{ip^j}{n} \equiv \binom{i}{\ell} \binom{m}{2}$ (mod p) and the *n*th coefficient is equivalent to $\sum_{i=0}^{p-1} \binom{i}{\ell}$ or $\binom{p}{\ell+1}$ modulo p. Thus, if n is not $(p-1)p^j$, then the *n*th coefficient is divisible by p. Thus, a complete factorization of $\lambda^{(p^n)} - 1$ is

$$\{\lambda - 1\} \bigcup \left\{ \sum_{i=0}^{p-1} \lambda^{(ip^j)} : j \in \{0, 1, \dots, n-1\} \right\}.$$

References

[1] Nathan Jacobson. Basic Algebra . W. H. Freemand and Company, New York, second edition, 1985.

- [2] Nathan Jacobson. Basic Algebra I. W. H. Freemand and Company, New York, second edition, 1989.
- [3] Marilynn Livingston and Quentin F. Stout. Perfect Dominating Sets. Proceedings of the Twenty-first Southeastern Conference on Combinatorics, Graph Theory, and Computing (Boca Raton, 1990). Congressus Numerantium, pages 187–203, 1990.