# Digraphs of Finite Linear Transformations

D. G. Hoffman
Auburn University

### Abstract

If $T$ is a function from a finite set $V$ to itself, we form the digraph $D$ of $T$ as follows. It has $V$ for its vertex set, and there is an arc from $x$ to $T(x)$ for each $x \in V$. Here we answer the following question. Given a finite field $F$, which digraphs arise as digraphs of a linear transformation from some finite dimensional vector space over $F$ to itself?

## 1 Introduction

What does a linear transformation from a vector space to itself really look like? Linear algebra provides a wonderful answer. The vector space is really a direct sum of quotient rings of the polynomial ring, and the transformation is really multiplication by $x$ in each summand; see Theorem 1 below. (This corresponds to finding a basis for which the matrix of the transformation is in rational canonical form.) Not only is this an esthetically satisfying answer, it is also a fundamental tool for attacking many problems, including the one we address here.

We seek a combinatorial answer. Given a finite field $F$, we will determine necessary and sufficient conditions on a digraph $D$ for the existence of a vector space $V$ over $F$, a linear transformation $T$ from $V$ to $V$, and a one-to-one correspondence from the vertices of $D$ onto $V$, so that for vertices $x$ and $y$, there is an arc from $x$ to $y$ if and only if $T(v)$ corresponds to $y$, where $v$ is the vector corresponding to $x$.

Our answer is quite different from the linear algebraists; but we are actually answering a different question, because we have a different equivalence relation on linear transformations in mind. For the linear algebraist, the relation is similarity; i.e. conjugation by a non-singular linear transformation. For us, the relation is conjugation by an arbitrary bijection.

## 2 Preliminaries

We denote by $\mathbb{P}$, $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ the positive integers, the non-negative integers, the integers and the rationals, respectively. Fixed throughout is a prime $p$, $\alpha \in \mathbb{P}$, and a field $F$ of order $q = p^\alpha$. All vector spaces are finite dimensional vector spaces over $F$.

We say $P = (V, T)$ is a *pair* if $V$ is a finite set, and $T : V \to V$. If further $V$ is a vector space, and $T$ is linear, then $P$ is a *linear pair*. If $P_1 = (V_1, T_1)$, $P_2 = (V_2, T_2)$ are pairs, we say that $P_1$ and $P_2$ are *conjugate* if for some bijection $\pi : V_1 \to V_2$, $\pi \circ T_1 = T_2 \circ \pi$. If further $P_1$ and $P_2$ are linear pairs, and such a linear $\pi$ can be found, then we say $P_1$ and $P_2$ are *similar*. Note that conjugacy is an equivalence relation on the class of pairs, and similarity is an equivalence relation on the class of linear pairs. We define the *direct sum* $P_1 \oplus P_2 = (V_1 \times V_2, T_1 \oplus T_2)$ as follows:

$$(T_1 \oplus T_2)(v_1, v_2) = (T_1(v_1), T_2(v_2)) \text{ for all } v_1 \in V_1, v_2 \in V_2.$$

We can obviously extend this definition to the direct sum of any finite number of pairs. Note that the direct sum of linear pairs is again linear.

If $P = (V, T)$ is a pair, we define the *digraph of* $P$, $D(P)$, as follows. $V$ is the vertex set of $D(P)$, and there is an arc from $v$ to $T(v)$ for every $v \in V$. (See [1] for our graph theory terminology.) Note that two pairs are conjugate if and only if their digraphs are isomorphic.

If $D_1$ and $D_2$ are digraphs on vertex sets $V_1$ and $V_2$ respectively, we define the digraph $D_1 \times D_2$ on vertex set $V_1 \times V_2$ as follows: there is an arc in $D_1 \times D_2$ from $(v_1, v_2)$ to $(w_1, w_2)$ if and only if there is an arc in $D_i$ from $v_i$ to $w_i$ for $i = 1, 2$. Note that for pairs $P_1$, $P_2$,

$$D(P_1 \oplus P_2) = D(P_1) \times D(P_2).$$

The above definition and formula can obviously be extended to any finite number of digraphs and pairs.

The digraph $D$ is said to be a *functional digraph* if it is the digraph of a pair. If further $D$ is the digraph of a linear pair, we say $D$ is a *linear digraph*. (Abstract note: if $D$ is isomorphic to a functional (resp. linear) digraph, then $D$ *is* a functional (resp. linear) digraph.)

We can now precisely state our goal here. It is to answer the following:

**Question:** *Which digraphs are linear?*

(The answer depends of course on the field $F$, which is fixed throughout this discussion.)

Before we begin our attack, we need to remind the reader of the structure of both functional digraphs and linear pairs. This we do in the next two sections.

# 3 Functional Digraphs

It is easy to determine if a given digraph is functional. We need only check that each vertex has out-degree 1. But we will need a more global description of functional digraphs.

Let $P = (V, T)$ be a pair, and $D = D(P)$ its digraph.

Let $V_1 = \{v \in V \mid \text{ for some } i \in \mathbb{P}, T^i(v) = v\}$, let $T_1$ be the function $T$ restricted to $V_1$ and let $P_1 = (V_1, T_1)$. We call $P_1$ the *invertible part* of $P$. Its digraph $D_1$ is a vertex disjoint union of directed cycles, and $T_1$ is a permutation of $V_1$. $D_1$ is the subdigraph of $D$ induced by all the vertices of $D$ contained in directed cycles. The rest of $D$ is obtained from $D_1$ by attaching to each vertex $v$ of $D_1$ a (possibly trivial) directed tree, each of whose arcs is directed towards $v$, as we now describe.

($\mathbf{R}$, $v$) is a *rooted tree* if $\mathbf{R}$ is a tree, (undirected), and $v$ is a vertex of $R$, called its *root*. For each $v \in V_1$, we define the rooted tree $(R, v)$ of $D$ at $v$ as follows: the vertices of $R$ are $\{v\} \cup \{w \in V \backslash V_1 \mid \text{ for some } i \in \mathbb{P}, T^i(w) = v\}$, and two vertices of $R$ are adjacent in $R$ if they are the ends of an arc of $D$. The resulting collection of rooted trees (one for each $v \in D_1$) is called the set of *rooted trees of $D$*; note that their vertex sets partition $V$. Note also that $D_1$, together with the set of rooted trees of $D$, completely determine $D$, and hence $P$.

# 4 Linear Pairs

The polynomial $f(x) \in F[x]$ is *monic* if it is not the zero polynomial, and its leading coefficient is 1. Given such an $f(x)$, we define the linear pair $[f(x)] = (V, T)$ as follows:

$$V = F[x]/\langle f(x) \rangle,$$

the quotient ring of the polynomial ring by the principal ideal $\langle f(x) \rangle$, and

$$T(g(x)) \equiv xg(x) \pmod{f(x)}, \text{ for all } g(x).$$

(See, for example, [3] for details and proofs of everything in this section.)

If $f(x) = (c(x))^e$, where $c(x)$ is an irreducible polynomial, and $e \in \mathbb{P}$, then the linear pair $[f(x)]$ is said to be *basic*.

There are many theorems in linear algebra which could be called "fundamental". This is our personal favorite:

**Theorem 1** *Every linear pair is similar to a direct sum of basic pairs. The representation is unique, up to the ordering of the summands.* □

# 5 An Initial Decomposition

So let $D$ be a digraph; we want to determine if $D$ is linear. Our first condition is obvious.

**Condition 1** *$D$ is a functional digraph.*

Our main goal in this section is to establish another condition, which will effectively divide our problem into two sub-problems.

A linear pair $(V, T)$ is said to be *nilpotent* if some power of $T$ is the zero transformation. Note that the digraph of a nilpotent pair consists of a single directed loop with a tree directed to it. On the other hand, $(V, T)$ is said to be *invertible* if $T$ is. Note that the digraph of an invertible pair is a vertex disjoint union of directed cycles.

**Theorem 2** *Every linear pair is similar to the direct sum of a nilpotent linear pair and an invertible linear pair.*

**Proof:** This is well known. We can prove it directly from Theorem 1. Write our given pair as the direct sum of basic pairs. The direct sum of basic summands of the form $[x^e]$ is nilpotent; the direct sum of the remaining summands is invertible. (By convention, the direct sum of no pairs at all is the pair whose digraph consists of a single directed loop.) □

So if $D$ is in fact linear, we must have $D$ isomorphic to $D_N \times D_I$, where $D_N$ is a tree directed to a single loop, and $D_I$ is the vertex disjoint union of directed cycles defined from $D$ in section 3. Hence:

**Condition 2** *The rooted trees of $D$ are pairwise isomorphic.*

(Two rooted trees are *isomorphic* if there is a bijection between the vertex sets which preserves adjacency, and takes the root of one to the root of the other.)

We have divided our main question into two:

**Question 1** *Let $D_N$ be a digraph consisting of a single tree directed to a directed loop. Is $D_N$ the digraph of a nilpotent linear pair?*

**Question 2** *Let $D_I$ be a digraph consisting of a vertex disjoint union of directed cycles. Is $D_I$ the digraph of an invertible linear pair?*

We address these questions in turn.

# 6 Nilpotent Pairs

Let $f$ be a function. If $c$ is in the range of $f$, we say that $f$ is *almost* $c$ if the set

$$\{x \mid x \text{ is in the domain of } f, \text{ and } f(x) \neq c\} \text{ is finite.}$$

We say $f$ is *almost constant* if it is almost $c$ for some $c$.

A function $\varphi$ from the class of linear pairs into $\mathbb{N}$ is said to be be *additive* if

$$\varphi(P_1 \oplus P_2) = \varphi(P_1) + \varphi(P_2)$$

for all linear pairs $P_1$, $P_2$.

In both the nilpotent case, and the invertible case, our attack will proceed like this:

First, we will define a set of additive functions. Next, we will compute the values of these functions on the basic pairs in question. Then we will compute the values of these functions on the hypothetical pair whose digraph is given; this will be possible because the functions we define will be conjugacy invariants, i.e., their values on a pair are determined by the digraph of the pair. Finally, we must find a multiset of basic pairs whose function values sum to the target values computed from the digraph; this is a matter of finding a solution in $\mathbb{N}$ to a system of linear equations.

If $P = (V, T)$ is a linear pair, and $i \in \mathbb{N}$, let $\eta(P, i)$ be the dimension of the null space of $T^i$. Note that for each fixed $i$, $\eta$ is additive in its first argument.

**Lemma 1** *Let $e \in \mathbb{P}$, $i \in \mathbb{N}$. Then*

$$\eta([x^e], i) = \min(e, i).$$

**Proof:** We may identify the elements of $F[x]/\langle x^e\rangle$ with the set of polynomials of degree less than $e$. Then the null space of $T^i$ is $W = \{f(x) \mid \deg f(x) < e, x^i f(x) \equiv 0(\bmod x^e)\}$. But $x^i f(x) \equiv 0(\bmod x^e)$ if and only if

$$x^{e-\min(e,i)} \text{ divides } f(x), \text{ so}$$

$$W = \{x^{e-\min(e,i)} g(x) \mid \deg g(x) < \min(e, i)\},$$

which has dimension $\min(e, i)$. □

Recall $D_N$ is a functional digraph consisting of a single tree directed to a directed loop. Let $(R, v)$ be the rooted tree of $D_N$. For each $n \in \mathbb{N}$, let $\ell(n)$ be the number of vertices of $R$ whose distance from $v$ is exactly $n$. Note that $\ell$ is almost zero. If $D_N$ is the digraph of a linear pair, $v$ must correspond to the zero vector. Thus we have:

**Condition 3** *For each $i \in \mathbb{N}$, there exists $d(i) \in \mathbb{N}$ with $\sum_{j=0}^{i} \ell(j) = q^{d(i)}$.*

Note that $d$ is almost constant, and that if $D_N$ is the digraph of a linear pair $P_N$, then $\eta(P_N, i) = d(i)$ for each $i \in \mathbb{N}$. Also, $d(0) = 0$.

Suppose that $P_N$ is the direct sum, over all $e \in \mathbb{P}$, of $y(e)$ copies of $[x^e]$. Thus $y$ is almost zero, and for all $i \in \mathbb{N}$,

$$(*) \qquad \sum_{e \in \mathbb{P}} y(e) \min(e, i) = d(i) \qquad (1)$$

by Lemma 1, and the additivity of $\eta$. A simple calculation shows that these equations determine the function $y$:

**Condition 4** *For each $e \in \mathbb{P}$,*

$$y(e) = 2d(e) - d(e-1) - d(e+1) \text{ is non-negative.}$$

(Since $d$ is almost constant, $y$, as defined in Condition 4, is almost zero.)

One more condition, and we are done with the nilpotent case.

**Condition 5** *$(R, v)$ is isomorphic to the rooted tree of the digraph of the direct sum over all $e \in \mathbb{P}$ of $y(e)$ copies of $[x^e]$.*

Obviously, $D_N$ is linear if and only if Conditions 3, 4 and 5 all hold.

Because the system $(*)$ uniquely determines the function $y$, we have the following:

**Corollary 1** *Two nilpotent linear pairs are conjugate if and only if they are similar.* □

## 7 Invertible Pairs - a Preliminary Decomposition

This case differs from the previous one in several respects. In the nilpotent case, the function $\ell$ defined on the digraph does not determine the digraph. The corresponding function here does, so there will be no need for a condition like Condition 5. Also, the analog of Corollary 1 is definitely false in this case. This is for two reasons. Firstly, in the nilpotent case, the values of the $\eta$ function for a basic pair determine the basic pair. The corresponding functions here do not have this property, that is Corollary 1 is false even for basic invertible pairs. Secondly, the system of equations here that correspond to $(*)$ does not have a unique solution.

If $\alpha, \beta$ are elements of a commutative ring $R$ with unity 1, let the *order of $\alpha$ (mod $\beta$)*, ord $(\alpha, \beta)$, be the smallest $k \in \mathbb{P}$ for which $\alpha^k - 1$ is in the principal ideal $\langle \beta \rangle$, if such $k$'s exist. And the *order of $\alpha$*, ord $(\alpha)$, is defined to be ord $(\alpha, 0)$.

We recall the Moebius function $\mu : \mathbb{P} \to \mathbb{Z}$:

If $n$ is divisible by the square of a prime, then $\mu(n) = 0$. If $n$ is the product of $k \in \mathbb{N}$ distinct primes, then $\mu(n) = (-1)^k$, so $\mu(1) = 1$. We need the following slight generalization of the Moebius inversion formula. The proof is the same as the usual proof the standard Moebius inversion formula, see for example [4].

**Theorem 3** *Let $A$ be a set of primes, let $B$ be the set of positive integers not divisible by any prime in $A$. Let $f$, $g : B \to \mathbb{Z}$. Then the following two statements are equivalent:*

*For all $b \in B$, $f(b) = \sum_{i|b} g(i)$.*

*For all $b \in B$, $g(b) = \sum_{i|b} f(i)\mu(\frac{b}{i})$.* □

(In both sums, the index $i$ ranges over all positive divisors of $b$.)

If $P = (V,T)$ is a linear pair, and $i \in \mathbb{R}$, let $\varphi(P,i)$ be the dimension of the null space of $T^i - I$, where $I$ is the identity map on $V$. Note that for each fixed $i$, $\varphi$ is additive in its first argument.

Let $c(x) \neq x$ be a monic irreducible polynomial in $F[x]$. Define the *type* of $c(x)$, $\tau(c(x))$, by $\tau(c(x)) =$ ord $(x, c(x))$. Note that if $\beta$ is any root of $c(x)$ in an extension of $F$, then ord $(\beta) = \tau(c(x))$.

**Lemma 2** *Let $r \in \mathbb{P}$. Then there is a monic irreducible polynomial $c(x) \neq x$ in $F[x]$ of type $r$ if and only if $p \nmid r$.*

**Proof:** If $c(x)$ is such a polynomial of degree $d$, then $r \mid q^d - 1$, so $p \nmid r$.

Conversely, if $p \nmid r$, let $d =$ ord $(q,r)$, and let $K$ be an extension of $F$ of degree $d$. Then the multiplication group $K^*$ of non-zero elements of $K$ has order $q^d - 1$, and is cyclic. Since $r \mid q^d - 1$, $K^*$ has an element $\beta$ of order $r$. Let $c(x)$ be the minimum polynomial of $\beta$ over $F$. □

**Lemma 3** *Let $c(x) \neq x$ be a monic irreducible polynomial in $F[x]$ of degree $d$ and type $\tau(c(x)) = r$.*

Then $d =$ ord $(q,r)$.

**Proof:** Let $k =$ ord $(q,r)$, let $K = F[x]/\langle c(x)\rangle$, let $\beta = \langle c(x)\rangle + x$, so $\beta$ is a root of $c(x)$ in $K$. The multiplicative group $K^*$ of non-zero elements of $K$ has order $q^d - 1$, and contains an element of order $r$. Thus $r \mid q^d - 1$, so $k \mid d$. In particular, $K$ has a subfield $L$ of order $q^k$ containing $F$. Since $K^*$ is a cyclic group, and $r \mid q^k - 1$, $L^*$ contains all the elements of order $r$ in $K^*$. In particular, $\beta \in L$, so $K = F(\beta) \subseteq L$. Thus $K = L$, and so $d = k$. □

**Lemma 4** *Let $e, s \in \mathbb{P}$, with $p \nmid s$, let $t \in \mathbb{N}$.*

Then

$$\varphi([(c(x))^e], sp^t) = \begin{cases} 0 & \text{if } r \nmid s \\ \text{ord } (q,r)\min(e,p^t) & \text{if } r \mid s \end{cases}$$

**Proof:** This is just like the proof of Lemma 1. We need to calculate the dimension of

$$W = \{f(x) \mid \deg f(x) < de, x^{sp^t} f(x) \equiv f(x) (\text{mod } (c(x))^e)\}.$$

(Here $d =$ ord $(q,r)$). But $x^{sp^t} f(x) \equiv f(x)$ (mod $(c(x))^e$) if and only if $f(x) \equiv 0$ (mod $(c(x))^e/g(x)$)), where $g(x) = gcd(x^{sp^t} - 1, (c(x))^e)$. Thus $W$ has dimension $\deg g(x)$.

Now $x^{sp^t} - 1$ has $s$ distinct roots, the $s^{th}$ roots or unity, each with multiplicity $p^t$.

And $(c(x))^e$ has $d$ distinct roots, each a primitive $r^{th}$ root of unity, and each with multiplicity $e$.

The result now follows by counting common roots, and using Lemma 3. □

We now turn to our digraph $D_I$, which is a vertex-disjoint union of directed cycles. Let $\lambda(i)$ denote the number of such cycles of length $i$, for each $i \in \mathbb{P}$. Note that $\lambda$ is almost 0.

For each $i \in \mathbb{P}$, let

$$\pi(i) = \sum_{j|i} j\lambda(j).$$

(Note that $\lambda$ may be recovered from $\pi$ by Theorem 3.)

Thus:

**Condition 6** *For each $i \in \mathbb{P}$, there is some $\delta(i) \in \mathbb{N}$ with $\pi(i) = q^{\delta(i)}$.*

This condition is necessary because if $D_I$ is the digraph of a linear pair $P_I$, then $\varphi(P_I, i) = \delta(i)$ for each $i \in \mathbb{P}$.

Let $S = \{i \in \mathbb{P} \mid \lambda(i) \neq 0\}$, let $n$ be the least common multiple of $S$. Note that $\pi$ and $\delta$ are periodic functions with period $n$. Also, write $n = mp^{t_0}$, $p \nmid m$.

**Lemma 5** *For fixed $s \in \mathbb{P}$, $p \nmid s$, $\pi(sp^t)$ is almost constant as a function of $t \in \mathbb{N}$. In fact, for $t \geq t_0$, $\pi(sp^t) = \pi(sp^{t_0})$ and $\delta(sp^t) = \delta(sp^{t_0})$.*

**Proof:** For $t \geq t_0$,

$$\pi(sp^t) = \sum_{s_1|s}\sum_{i=0}^{t} s_1p^i\lambda(s_1p^i) = \sum_{s_1|s}\sum_{i=0}^{t_0} s_1p^i\lambda(s_1p^i) = \pi(sp^{t_0}).$$

The second equality is due to the fact that for $t > t_0$, $\lambda(s_1p^t) = 0$. □

Suppose $D_I$ is the digraph of the linear pair $P_I$, which is a direct sum of basic pairs. For each $s$, $e \in \mathbb{P}$, with $p \nmid s$, let $x_s(e)$ denote the number of summands of the form $[c(x)^e]$, where $c(x)$ has type $s$. So by the additivity of $\varphi$, and Lemmata 3 and 4, we have

$$\sum_{r|s} \text{ord }(q,r)\sum_{e\in\mathbb{P}} \min(e,p^t)x_r(e) = \delta(sp^t)$$

$$\text{for all } s \in \mathbb{P}, p \nmid s, \text{ and } t \in \mathbb{N}.$$

Writing

$$(**) \qquad \rho_s(t) = \sum_{e\in\mathbb{P}} \min(e,p^t)x_s(e) \quad \text{for all } s \in \mathbb{P}, p \nmid s, t \in \mathbb{N}, \qquad (2)$$

we have, using Theorem 3 with $A = \{p\}$:

**Condition 7** *For all $s \in \mathbb{P}$, $p \nmid s$, and for all $t \in \mathbb{N}$, there exists $\rho_s(t) \in \mathbb{Z}$ satisfying*

$$\sum_{r|s} \delta(rp^t)\mu(\frac{s}{r}) = \textit{ord }(q,s)\rho_s(t).$$

Note that for fixed $s$, $\rho_s(t)$ is almost constant as a function of $t$. Indeed, $\rho_s(t) = \rho_s(t_0)$ for $t \geq t_0$.

There remains the problem of solving the system $(**)$ for the unknowns $x_s(e) \in \mathbb{N}$; this we address in the next section.

# 8 A System of Linear Equations Over $\mathbb{N}$

Let $a_0, a_1, \ldots$ be an infinite increasing sequence of integers, with $a_0 = 1$.

For each $x : \mathbb{P} \to \mathbb{Z}$, almost 0, define $\hat{x} : \mathbb{N} \to \mathbb{Z}$ by

$$\hat{x}(t) = \sum_{e \in \mathbb{P}} \min(e, a_t) x(e).$$

Note that $\hat{x}$ is almost $\sum_{e \in \mathbb{P}} ex(e)$.

**Theorem 4** *Let $\rho : \mathbb{N} \to \mathbb{Z}$ be almost constant. Then there is a function $x : \mathbb{P} \to \mathbb{N}$, almost 0, with $\hat{x} = \rho$, if and only if*

$$\lceil \theta(t+1) \rceil \leq \lfloor \theta(t) \rfloor \textit{ for all } t \in \mathbb{N},$$

*where $\theta(0) = \rho(0)$, and for $t \in \mathbb{P}$,*

$$\theta(t) = \frac{\rho(t) - \rho(t-1)}{a_t - a_{t-1}}.$$

Here $\lfloor x \rfloor$ (respectively $\lceil x \rceil$) denotes the greatest (respectively, the least) integer less (respectively greater) than or equal to the rational number $x$.

We devote the rest of this section to proving Theorem 4.

For each $t \in \mathbb{P}$, let $I_t = \{e \in \mathbb{P} \mid a_{t-1} < e < a_t\}$. If $x : \mathbb{P} \to \mathbb{N}$, almost 0, we say $x$ is *sparse*, if for all $t \in \mathbb{P}$, $\sum_{e \in I_t} x(e) \leq 1$.

For each $a$, $e \in \mathbb{P}$, let

$$\epsilon_a(e) = \begin{cases} -1 & \text{if } e = a \\ 1 & \text{if } e = a+1 \\ 0 & \text{otherwise.} \end{cases}$$

Note that for $t \in \mathbb{N}$,

$$\hat{\epsilon}_a(t) = \begin{cases} 1 & \text{if } a < a_t \\ 0 & \text{otherwise} \end{cases}$$

In particular, if $a$, $b \in I_t$ for some $t$, then $\hat{\epsilon}_b - \hat{\epsilon}_{a-1}$ is the zero function.

If $x : \mathbb{P} \to \mathbb{N}$, almost 0, and not sparse, we may *adjust* $x$ to a function $x'$ as follows. Choose $t$ with

$$\sum_{e \in I_t} x(e) \geq 2,$$

let $Y = \{e \in I_t \mid x(e) \neq 0\}$, let $a$ and $b$ be (respectively) the smallest and largest elements of $Y$, and let

$$x' = x + \epsilon_b - \epsilon_{a-1}.$$

Note that $\hat{x'} = \hat{x}$. Also, only a finite sequence of adjustments can be performed, starting with $x$. And the resulting function $x''$ is sparse and satisfies $\hat{x''} = \hat{x}$. So the existence of the function $x$ in the statement of Theorem 4 is equivalent to the existence of a sparse $x$.

We now describe our unknown sparse $x$ in terms of other unknowns:

$$\text{Let } K = \{t \in \mathbb{P} \mid \sum_{e \in I_t} x(e) = 1\}.$$

For each $t \in K$, let $e_t$ be the unique element of $I_t$ with $x(e_t) = 1$. (And if $t \notin K$, let $e_t = a_{t-1}$.)

For each $t \in \mathbb{N}$, let $y(t) = x(a_t)$.

And our system of equations now is

$$(***) \qquad \text{for all } t \in \mathbb{N}, \qquad \sum_{\ell \in \mathbb{N}} y(\ell) \min(a_\ell, a_t) + \sum_{\ell \in K} \min(e_\ell, a_t) = \rho(t). \qquad (3)$$

But this system $(***)$ has a unique solution, which we derive.

Note $\theta(0) = \sum_{\ell \in \mathbb{N}} y(\ell) + |K|$,

$$\text{and for } t \in \mathbb{P}, \quad \theta(t) = \sum_{\ell \geq t} y(\ell) + |\{k \in K \mid k > t\}| + \frac{e_t - a_{t-1}}{a_t - a_{t-1}}.$$

But $0 \leq \frac{e_t - a_{t-1}}{a_t - a_{t-1}} < 1$, with strict inequality if and only if $t \in K$. Thus $K = \{t \in \mathbb{P} \mid \theta(t) \notin \mathbb{Z}\}$, and for each $t \in K$, $e_t = a_{t-1} + (a_t - a_{t-1})(\theta_t - \lfloor \theta_t \rfloor)$. Also, for all $t \in \mathbb{N}$,

$$\begin{aligned} \lfloor \theta(t) \rfloor &= \sum_{\ell \geq t} y(t) + \mid \{k \in K \mid k > t\} \mid, \text{ and} \\ \lceil \theta(t) \rceil &= \sum_{\ell \geq t} y(\ell) + \mid \{k \in K \mid k \geq t\} \mid . \end{aligned}$$

Hence $\lfloor \theta(t) \rfloor - \lceil \theta(t+1) \rceil = y(t) \in \mathbb{N}$, and so the conditions on $\theta$ in Theorem 4 are necessary for a solution. To show sufficiency, we need only verify that the $K$, $e_t$, and $y$ we derived from $(***)$ actually satisfy $(***)$.

Since $\rho$ is almost constant, $\theta$ is almost 0, so $K$ is finite and $y$ is almost 0. (Thus our sparse $x$ is almost 0.)

For $t \in \mathbb{N}$, let $\epsilon_t = \theta_t - \lfloor \theta_t \rfloor$. If $t \in K$, then $0 < \epsilon_t < 1$, so $e_t \in I_t$.

Let $t \in \mathbb{N}$, we proceed to prove $(***)$. For $i \in \mathbb{N}$, we define

$$[i] = \begin{cases} 1 & \text{if } i \in K \\ 0 & \text{if } i \notin K. \end{cases}$$

Here is the unpleasant calculation:

$$\sum_{\ell\in\mathbb{N}} y(\ell)\min(a_\ell,a_t)+\sum_{\ell\in K}\min(e_\ell,a_t)=$$

$$\sum_{\ell=0}^{t} a_\ell(\theta(\ell)-\theta(\ell+1)-\epsilon_\ell+\epsilon_{\ell+1}-[\ell+1])+$$

$$a_t\sum_{\ell=t+1}^{\infty}(\theta(\ell)-\theta(\ell+1)-\epsilon_\ell+\epsilon_{\ell+1}-[\ell+1])+$$

$$\sum_{\ell=1}^{t}[\mathrm{e}](a_{\ell-1}+(a_\ell-a_{\ell-1})\epsilon_\ell)+$$

$$a_t\sum_{\ell=t+1}^{\infty}[\ell]=$$

$$\sum_{\ell=0}^{t} a_\ell\theta(\ell)-\sum_{\ell=1}^{t+1} a_{\ell-1}\theta(\ell)+a_t\theta(t+1)$$

$$-\sum_{\ell=0}^{t} a_\ell\epsilon_\ell+\sum_{\ell=1}^{t+1} a_{\ell-1}\epsilon_\ell-a_t\epsilon_{t+1}$$

$$+\sum_{\ell=1}^{t}[\ell](a_\ell-a_{\ell-1})\epsilon_\ell-\sum_{\ell=1}^{t+1} a_{\ell-1}[\ell]$$

$$-a_t\sum_{\ell=t+2}^{\infty}[\ell]+\sum_{\ell=1}^{t} a_{\ell-1}[\ell]+a_t\sum_{\ell=t+1}^{\infty}[\ell]=$$

$$\rho(0)+\sum_{\ell=1}^{t}(\rho(\ell)-\rho(\ell-1))=\rho(t).$$

In the above calculation, we used the following facts:

$$y(\ell)=\theta(\ell)-\theta(\ell+1)-\epsilon_\ell+\epsilon_{\ell+1}-[\ell+1];$$

and $[\ell]\epsilon_\ell=\epsilon_\ell$, for $\ell\in\mathbb{N}$.

This concludes the proof of Theorem 4.

For each $s\in\mathbb{P}$ with $p\nmid s$, we apply this theorem to $(**)$ with $\rho=\rho_s$, $a_t=p^t$:

**Condition 8** *For each $s\in\mathbb{P}$ with $p\nmid s$, and for all $t\in\mathbb{N}$, $\lceil\theta_s(t+1)\rceil\le\lfloor\theta_s(t)\rfloor$; where $\theta_s(0)=\rho_s(0)$, and for $t\in\mathbb{P}$,*

$$\theta_s(t)=\frac{\rho_s(t)-\rho_s(t-1)}{p^t-p^{t-1}}.$$

And these are all the conditions!

# 9 But Is It an Algorithm?

Many of these conditions seem to take an infinite amount of checking. But this is an illusion.

For example, suppose $\ell(j) = 0$ for $j > j_0$. Then Condition 3 only needs to be checked for $i \leq j_0$, and Condition 4 only for $e \leq j_0$. (This further insures that the direct sum in Condition 5 is a finite one.)

Also concerning Condition 5, there is the matter of determining if two rooted trees are isomorphic. There is an efficient algorithm for this problem, which seems to have been independently discovered many times over; see [2] for an interesting history.

Recall that in Section 7 we defined $n$ to be the lcm of the set $S$ of cycle lengths of the given permutation, i.e. $n$ is the order of the permutation. And $n = mp^{t_0}$, $p \nmid m$.

Since $\pi(i) = \pi(\text{lcm } \{j \in S \mid j|i\})$, Condition 6 need only be checked for $i|n$. And the same formula can be used to prove the following:

**Lemma 6** *Let $p_1 \neq p$ be a prime, $k \in \mathbb{P}$, with $p_1^k \nmid n$. For the function $\delta$ defined by Condition 6, $\delta(p_1^k x) = \delta(p_1^{k-1} x)$ for all $x \in \mathbb{P}$.* □

Conditions 7 and 8 range over all $s \in \mathbb{P}$, $p \nmid s$, and all $t \in \mathbb{N}$. Certainly we can restrict ourselves to $t \leq t_0$. And the following theorem shows that we need only check those $s$ which divide $m$.

**Theorem 5** *Suppose Condition 7 holds, defining $\rho_s(t)$. Then $\rho_s(t) = 0$ if $s \nmid m$.*

**Proof:** We need only show that

$$\sum_{r|s} \delta(rp^t)\mu(\frac{s}{r}) = 0.$$

Since $s \nmid m$, we can find a prime $p_1 \neq p$, and $k \in \mathbb{P}$, with $s = s_1 p_1^k$, $p_1 \nmid s_1$, $p_1^k \nmid m$. Then

$$\begin{aligned}
\sum_{r|s} \delta(rp^t)\mu(\frac{s}{r}) &= \sum_{i|s_1}\sum_{j=0}^{k} \delta(ip_1^j p^t)\mu(\frac{s_1 p_1^k}{ip_1^j}) \\
&= \sum_{i|s_1}\sum_{j=k-1}^{k} \delta(ip_1^j p^t)\mu(\frac{s_1}{i})\mu(p_1^{k-j}) \\
&= \sum_{i|s_1} (\delta(ip_1^k p^t)\mu(\frac{s_1}{i}) - \delta(ip_1^{k-1} p^t)\mu(\frac{s_1}{i})).
\end{aligned}$$

But every summand of this last sum is zero by Lemma 6. □

Thus Conditions 7 and 8 need only be checked for those $s$, $t$ with $sp^t \mid n$. In particular, the resulting direct sum of basic pairs constructed only involves finitely many basic pairs.

## Acknowledgements

The author presented this paper at the $19^{th}$ Australasian Conference on Combinatorial Mathematics and Combinatorial Computing at the University of Adelaide, while he was a Raybould Fellow at the University of Queensland. He is grateful to both universities for their support and hospitality.

## References

[1] Bondy and Murty, Graph Theory with Application, North-Holland, 1976.

[2] Charles J. Colbourn and Kelloggs Booth, Linear Time Automorphism Algorithms for Trees, Interval Graphs and Planar Graphs, SIAM Journal of Computation, Vol. 10 No. 1, 1981, 203-225.

[3] I. N. Herstein, Topics in Algebra, Blaisdell, 1964.

[4] W. J. Le Veque, Fundamentals of Number Theory, Addison-Wesley, 1977.

*(Received 14/2/95)*