Combinatorics, Probability and Computing (2002) 11, 35–42. Printed in the United Kingdom
DOI: 10.1017/S0963548301004874

Distinct Sums Modulo *n* and Tree Embeddings

ANDRÉ E. KÉZDY[1] and HUNTER S. SNEVILY[2]

[1] Department of Mathematics,
University of Louisville, Louisville, KY 40292, USA
(e-mail: kezdy@louisville.edu)

[2] Department of Mathematics,
University of Idaho, Moscow, ID 83844, USA
(e-mail: snevily@uidaho.edu)

Received 11 July 2000; revised 6 March 2001

In this paper we are concerned with the following conjecture.

Conjecture. For any positive integers n and k satisfying $k < n$, and any sequence $a_1, a_2, \ldots, a_k$ of not necessarily distinct elements of Z_n, there exists a permutation $\pi \in S_k$ such that the elements $a_{\pi(i)} + i$ are all distinct modulo n.

We prove this conjecture when $2k \leqslant n+1$. We then apply this result to tree embeddings. Specifically, we show that, if T is a tree with n edges and radius r, then T decomposes K_t for some $t \leqslant 32(2r+4)n^2 + 1$.

1. Introduction

In this paper we are concerned with the following conjecture, which is a reformulation of Conjecture 4 in the paper by Snevily [10].

Conjecture 1.1. *For any positive integers n and k satisfying $k < n$, and any sequence $a_1, a_2, \ldots, a_k$ of not necessarily distinct elements of Z_n, there exists a permutation $\pi \in S_k$ such that the elements $a_{\pi(i)} + i$ are all distinct modulo n.*

If true, Conjecture 1.1 would be sharp because, as is well known, the Cayley table Z_{2m} has no latin transversal, so the desired permutation may not exist when $k = n$. In fact Hall [4] resolved the $k = n$ case in abelian groups by showing that, for any sequence $a_1, \ldots, a_n$ of not necessarily distinct elements of an abelian group G of order n satisfying the obvious necessary condition that $\sum_{i=1}^{n} a_i = 0$, there are two permutations π and σ of the elements of $G = \{g_1, \ldots, g_n\}$ such that $\pi(g_i) - \sigma(g_i) = a_i$, for all $i = 1, \ldots, n$.

Hall's result also establishes the $k = n-1$ case of Conjecture 1.1 since, given $a_1, \dots, a_{n-1}$, one can set $a_n = -\sum_{i=1}^{n-1} a_i$ and apply Hall's theorem to obtain a permutation π such that $a_1 + \pi(1), \dots, a_n + \pi(n)$ are all distinct modulo n. Now, increasing all $\pi(i)$'s by the same constant, one can guarantee that $\pi(n) = 0$.

Conjecture 1.1 is related to several well-studied problems: latin transversals, cyclic neofields, combinatorial designs, and permutation groups. The $k = n-1$ case is particularly intriguing as it is closely related to N-permutations, which in turn are related to cyclic neofields. Constructions of the latter two objects have been accomplished using both number-theoretic and combinatorial methods. For more information on these topics, the reader is referred to the book by Hsu [5].

Alon [2] proved a result more general than Conjecture 1.1 when n is a prime, using polynomial methods. Using similar methods we prove the conjecture for all n when $2k \leqslant n + 1$. We then apply this result to tree embeddings.

A *decomposition* of a graph $G = (V, E)$ is a partition of E into pairwise edge-disjoint subgraphs. If these edge-disjoint subgraphs are all isomorphic to the same graph H, then we say that H *decomposes* G. One of the most famous conjectures about decomposing graphs is Ringel's conjecture [7], which states that every tree on n edges decomposes the complete graph on $2n + 1$ vertices, K_{2n+1}. Ringel's conjecture remains open. We can view the conjecture as an extremal problem by defining, for any tree T, a value $h(T)$ that equals the smallest positive integer m such that T decomposes K_m. The existence of $h(T)$ follows from a general theorem due to Wilson [13] that applies to all graphs. As a consequence of recent work by Yuster [12], $h(T) = O(n^{10})$, for any tree T with n edges. If one defines the function $g(n) = \max\{h(T) : T \text{ is a tree with } n \text{ edges}\}$, then Ringel's conjecture, if true, would show that $g(n) \leqslant 2n + 1$. In this paper we apply the proof of Conjecture 1.1 when $2k \leqslant n + 1$ to prove that, if T is a tree with n edges and radius r, then $h(T) \leqslant 32(2r + 4)n^2 + 1$. It follows that $g(n) = O(n^3)$.

2. Distinct sums modulo *n*

In this section we prove a theorem that is the foundation of our tree embedding technique appearing in the next section. First we introduce some notation.

Suppose n is a positive integer. We use $[n]$ as an abbreviation for the set $\{1, \dots, n\}$. The set of permutations of $[n]$ is denoted by S_n. A permutation $\pi \in S_n$ is viewed as the linear arrangement $\pi(1), \pi(2), \dots, \pi(n)$. We call this sequence the *sequence representation* of π. We shall omit commas from this sequence when doing so produces no ambiguity. For $i, j \in [n]$ and $\pi \in S_n$, define the *distance* from i to j in π to be $d_\pi(i, j) := \pi^{-1}(j) - \pi^{-1}(i)$. Clearly $d_\pi(i, j) = -d_\pi(j, i)$ and $-(n-1) \leqslant d_\pi(i, j) \leqslant n - 1$. For example, if π is the permutation 532687941, then $d_\pi(5, 6) = 3$, whereas $d_\pi(1, 8) = -4$.

A basic problem we address in this section is the following. Suppose that k is a positive integer and that we are given, for every unordered pair of elements $\{i, j\}$ from $[k]$, a number f_{ij} that represents a 'forbidden distance' between i and j. Is there a permutation $\pi \in S_k$ that avoids all of these forbidden distances? The answer is 'yes', as Lemma 2.2 shows. To prove this we make use of the following result.

Theorem 2.1 (Alon [1]). *Let F be an arbitrary field, and let $f = f(x_1, \ldots, x_n)$ be a polynomial in $F[x_1, \ldots, x_n]$. Suppose the degree of f is $\sum_{i=1}^{n} t_i$, where each t_i is a nonnegative integer. If the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ in f is nonzero, then, for any subsets $S_1, S_2, \ldots, S_n$ of F satisfying $|S_i| > t_i$, there are elements $s_1 \in S_1, s_2 \in S_2, \ldots, s_n \in S_n$ such that*

$$f(s_1, s_2, \ldots, s_n) \neq 0.$$

Our first lemma is a direct application of Theorem 2.1. We first proved Lemma 2.2 using the Alon–Tarsi lemma (see [3]) and multilinear polynomials. We then realized that our argument could be simplified if we used Theorem 2.1; this resulted in our proofs being very similar to those given in [2].

Lemma 2.2. *For any positive integer k and any assignment of forbidden distances f_{ij} to the unordered pairs from $[k]$, there exists a permutation $\pi \in S_k$ such that*

$$d_\pi(i,j) \neq f_{ij}, \quad \textit{for all } 1 \leqslant i < j \leqslant k. \tag{2.1}$$

Proof. Introduce k variables x_i for $1 \leqslant i \leqslant k$, where x_i represents the position that element i occupies in the sequence representation of a permutation of $[k]$. Now consider the following polynomial with k variables over the reals:

$$P(x_1, \ldots, x_k) = \prod_{1 \leqslant i < j \leqslant k} (x_i - x_j) \prod_{1 \leqslant i < j \leqslant k} ((x_i - x_j) - f_{ij}). \tag{2.2}$$

There is a permutation $\pi \in S_k$ satisfying (2.1) if and only if $P(x_1, \ldots, x_k) \neq 0$ for some $(x_1, \ldots, x_k) \in \{1, \ldots, k\}^k$.

The coefficient of the monomial $\prod_{i=1}^{k} x_i^{k-1}$ in P is the same as the coefficient of this monomial in the polynomial

$$\prod_{1 \leqslant i < j \leqslant k} (x_i - x_j) \prod_{1 \leqslant i < j \leqslant k} (x_i - x_j)$$

because the total degree of P is $k(k-1)$. Applying the Vandermonde identity

$$\prod_{1 \leqslant i < j \leqslant k} (x_i - x_j) = \sum_{\pi \in S_k} (-1)^{\mathrm{sign}(\pi)} \prod_{i=1}^{k} x_{\pi(i)}^{k-i},$$

one finds that this coefficient is $(-1)^{\binom{k}{2}} k!$.

Applying Theorem 2.1 to P with $S_1 = S_2 = \cdots = S_k = [k]$, it follows that there is some $(x_1, \ldots, x_k) \in [k]^k$ such that $P(x_1, x_2, \ldots, x_k) \neq 0$, which implies the existence of the desired permutation. □

Lemma 2.2 is sharp in the sense that, if $f_{ij} = 1$ for all $1 \leqslant i < j \leqslant k$, then a unique permutation π satisfies (2.1), namely the permutation with sequence representation $k(k-1) \cdots 21$.

Lemma 2.2 can be viewed as a generalization of Redei's theorem. Recall that a *tournament* is a complete graph whose edges have all been given an orientation. Redei's theorem states that every tournament contains a directed path visiting each vertex exactly once. If one considers the directed edge uv in the tournament as equivalent to forbidding the distance $f_{vu} = 1$, then Redei's theorem can be derived from Lemma 2.2. Essentially, Redei's theorem is equivalent to Lemma 2.2 in which the forbidden distances are restricted to values from the set $\{-1, 0, 1\}$. Despite the fact that Redei's theorem has relatively straightforward combinatorial proofs, we have not found a combinatorial proof of Lemma 2.2, even in the case in which the forbidden distances are restricted to values from the set $\{-2, -1, 0, 1, 2\}$.

A strengthening of Lemma 2.2 is possible using an observation that Alon [2] made, that the coefficient $(-1)^{\binom{k}{2}}k!$ of the monomial $\prod_{i=1}^{k} x_i^{k-1}$ in the expansion of (2.2) is nonzero modulo a prime p. We include the argument here for completeness. Let Z_n denote the group of integers modulo n under addition. A function $f : [k] \times [k] \to Z_n$ is *alternating* if $f(i, j) \equiv -f(j, i) \pmod{n}$, for all $i, j \in [k]$.

Lemma 2.3. *For any positive integers k and p satisfying $k < p$, p a prime, and any alternating function $f : [k] \times [k] \to Z_p$, there exists a permutation $\pi \in S_k$ such that*

$$d_\pi(i, j) \not\equiv f(i, j) \pmod{p}, \quad \textit{for all distinct } i, j \in [k]. \tag{2.3}$$

Proof. As in the previous proof, introduce k variables x_i for $1 \leqslant i \leqslant k$, where x_i represents the position that element i occupies in the sequence representation of a permutation of $[k]$. Now consider the following polynomial over the field Z_p:

$$P(x_1, \ldots, x_k) = \prod_{1 \leqslant i < j \leqslant k} (x_i - x_j) \prod_{1 \leqslant i < j \leqslant k} ((x_i - x_j) - f(i, j)). \tag{2.4}$$

There is a permutation $\pi \in S_k$ satisfying (2.3) if and only if

$$P(x_1, \ldots, x_k) \not\equiv 0 \pmod{p},$$

for some $(x_1, \ldots, x_k) \in \{1, \ldots, k\}^k$.

Now $P \not\equiv 0$ because the coefficient of the monomial $\prod_{i=1}^{k} x_i^{k-1}$ in P_1 is $(-1)^{\binom{k}{2}}k!$ which is not zero modulo p. It follows from Theorem 2.1 that there is some $(x_1, \ldots, x_k) \in \{1, \ldots, k\}^k$ such that $P(x_1, \ldots, x_k) \not\equiv 0 \pmod{p}$. □

We conjecture the following strengthening of Lemma 2.3.

Conjecture 2.4. *For any positive integers k and n satisfying $k < n$, and any alternating function $f : [k] \times [k] \to Z_n$, there exists a permutation $\pi \in S_k$ such that*

$$d_\pi(i, j) \not\equiv f(i, j) \pmod{n}, \quad \textit{for all distinct } i, j \in [k].$$

Conjecture 2.4, if true, would imply Conjecture 1.1 (by appropriately modifying the proof of Theorem 2.5). The following is the main tool used in the next section.

Theorem 2.5. *Let n and k be positive integers satisfying $2k \leqslant n + 1$. For any sequence $a_1, a_2, \ldots, a_k$ of not necessarily distinct elements of Z_n, there exists a permutation $\pi \in S_k$ such that the elements $a_{\pi(i)} + i$ are all distinct modulo n.*

Proof. It suffices to prove that there exists a permutation $\pi \in S_k$ such that

$$a_i - a_j + \pi(i) - \pi(j) \not\equiv 0 \ (\mathrm{mod}\ n), \quad \text{for all } i < j.$$

Because $|\pi(i) - \pi(j)| < n/2$ for all $\pi \in S_k$, there is a unique multiple n_{ij} of n such that, for any π, if $a_i - a_j + \pi(i) - \pi(j)$ is a multiple of n, then it is equal to n_{ij}. Lemma 2.2 now guarantees the desired permutation. □

We close this section with some conjectures. For $\mathbf{a} = (a_1, \ldots, a_k) \in Z_n^k$, let $\Phi(n, \mathbf{a})$ denote the number of permutations $\pi \in S_k$ such that the sums $a_{\pi(i)} + i$ are all distinct modulo n. Define $N(n,k) = \min_{\mathbf{a} \in Z_n^k} \Phi(n, \mathbf{a})$. Note that Conjecture 1.1 is equivalent to proving that $N(n,k) > 0$, for all positive integers k and n satisfying $k < n$. We conjecture that $N(n,k)$ is monotone for fixed n; that is, $N(n,k) \leqslant N(n,k+1)$ for all n and k satisfying $0 < k < n-1$. We also conjecture that $N(n,k)$ is monotone for fixed k; that is, $N(n,k) \leqslant N(n+1,k)$, for all n and k satisfying $0 < k < n$. In addition, we make these two conjectures about specific values of $N(n,k)$.

Conjecture 2.6. *If n is sufficiently large with respect to k, then*

$$N(n,k) = \begin{cases} (\frac{k}{2}!)^2, & \textit{if } k \textit{ is even,} \\ \lceil \frac{k}{2} \rceil (\lfloor \frac{k}{2} \rfloor !)^2, & \textit{if } k \textit{ is odd.} \end{cases}$$

Note that, if true, Conjecture 2.6 would be sharp because the vector

$$(\underbrace{0, \ldots, 0}_{\lfloor \frac{k}{2} \rfloor \text{ times}}, \underbrace{n-1, \ldots, n-1}_{\lceil \frac{k}{2} \rceil \text{ times}})$$

achieves the bound.

It is necessary to include the condition that n is sufficiently large with respect to k because, when k is near n, the values of $N(n,k)$ are smaller than those conjectured in Conjecture 2.6 (see Table 1).

Table 1 Values of $N(n,k)$ for $3 \leqslant n \leqslant 9$

$n \backslash k$	2	3	4	5	6	7	8
3	1	-	-	-	-	-	-
4	1	2	-	-	-	-	-
5	1	2	3	-	-	-	-
6	1	2	4	8	-	-	-
7	1	2	4	12	19	-	-
8	1	2	4	12	32	64	-
9	1	2	4	12	36	144	225

In light of the apparent monotonicity of $N(n,k)$, a particularly interesting case occurs when $k = n - 1$.

Conjecture 2.7. *For $n \geqslant 3$, $N(n, n-1)$ is equal to the number of cyclic neofields of order $n+1$.*

We do not define cyclic neofields here, but refer the reader to the book by Hsu [5].

3. A decomposition

In this section we show how to decompose a 'small' complete graph into edge-disjoint copies of a given tree. Our decomposition method relies heavily on Theorem 2.5.

Let $G = (V, E)$ be a connected graph. The *distance* between the vertex u and the vertex v in G, denoted $d_G(u, v)$, is the number of edges in a shortest path connecting u and v. Recall that the *eccentricity* of the vertex $v \in V(G)$, denoted $e(v)$, is defined to be $\max\{d_G(u, v) : u \in V\}$. The *radius* of G, $r(G)$ is the minimum eccentricity of its vertices. A vertex v is a *central vertex* of G if $e(v) = r(G)$.

Theorem 3.1. *If T is a tree with n edges and radius r, then T decomposes K_p, for some $p \leqslant 32(2r+4)n^2 + 1$.*

Proof. Let T be a tree that has n edges and radius r. Let v be a central vertex of T and x a vertex of T that is the maximum distance from v. Consider a new tree T' obtained from two disjoint copies T_1 and T_2 of T by identifying x_1 and v_2. Note that T' has $2n$ edges and the eccentricity of v_1 in T' is $2r$. Clearly T decomposes a given complete graph if T' does. This initial tree-duplicating step is required to guarantee that we work with a tree in which, for all k, the number of edges of the tree at distance k from v_1 is at most half the total number of edges.

Let $C_{4s}(t)$ denote the graph obtained from the cycle C_{4s} by blowing up each vertex to t vertices. Because $C_{4s}(t)$ is isomorphic to the weak tensor product of C_{4s} and $K_{t,t}$, it follows from work by Snevily [9] and Rosa [8] that $C_{4s}(t)$ decomposes the complete graph K_{8st^2+1}. We are interested in $C_{4s}(2n)$, where s is the smallest positive integer satisfying $4s \geqslant 2r+1$. Because $C_{4s}(2n)$ decomposes the complete graph K_{32sn^2+1}, it suffices to show that T' decomposes $C_{4s}(2n)$.

The vertices of $C_{4s}(2n)$ may be viewed as ordered pairs (i, j) $(0 \leqslant i < 2n,\ 0 \leqslant j < 4s)$ such that edges are pairs $(i, j)(i', j')$ satisfying $|j - j'| \equiv 1 \pmod{4s}$. Edges can naturally be thought of as having an angle. By an *embedding* of T into $C_{4s}(2n)$ we mean an injection of $V(T)$ into $V(C_{4s}(2n)$ that preserves adjacency.

To show T' decomposes $C_{4s}(2n)$, it is enough to demonstrate that one can embed T' into $C_{4s}(2n)$ so that every edge has a different angle, since the $4s \times 2n$ rotations of this embedding then clearly decompose $C_{4s}(2n)$. The remainder of the proof demonstrates how to perform this embedding of T'.

We view the tree T' as being rooted at v_1. Define the *level sets* $V_i = \{u \in V(T') : d(u, v_1) = i\}$, for $i = 0, \dots, 2r$. By definition, each V_i is nonempty and the V_is partition the vertices of T'. Because T' is a tree, each V_i induces an independent set. In particular, edges of T' have endpoints in consecutive level sets. For $i = 1, \dots, 2r$, let E_i denote the set of edges in the graph induced by $V_{i-1} \cup V_i$, and set $e_i = |E_i|$. Clearly $e_i > 0$, for all i, and $\sum_{i=1}^{2r} e_i = 2n$. By construction, we have $e_i \leqslant n$, for all i.

For $i = 1, \ldots, 2r$, define the *label set* L_i to be the set of e_i consecutive elements of Z_{2n} beginning at $m_i := \sum_{j=1}^{i-1} e_j$ (where $m_1 = 0$); so $L_1 = \{0, \ldots, e_1 - 1\}$ and $L_i := \{m_i, \ldots, m_i + e_i - 1\}$. By definition the L_is form a partition of $\{0, \ldots, 2n-1\}$. For any $f : V(T') \to Z_{2n}$, define $f(E_i) = \{f(b) - f(a) \bmod 2n : ab \in E_i, a \in V_{i-1}, b \in V_i\}$.

The desired embedding of T' will follow from a labelling $f : V(T') \to Z_{2n}$ satisfying all of the following:

(a) $f(v_1) = 0$,
(b) $f(E_i) = L_i$, for all $i = 1, \ldots, 2r$,
(c) $f|V_i$ is one-to-one, for all $i = 1, \ldots, 2r$.

We construct f by induction on i. Initially $f(v_1) = 0$. Now suppose that f has been defined on all level sets $V_0, \ldots, V_{i-1}$, for some $1 \leqslant i < 2r$, so that (a), (b) and (c) are all satisfied on the current domain of f. We must now show how to extend f to V_i. For convenience set $k = e_i \leqslant n$. Consider the edges $E_i = \{x_j y_j\}_{j=1}^{k}$. The sequence $f(x_1), \ldots, f(x_k)$ consists of not necessarily distinct values of Z_{2n}. Because $k \leqslant n$, Theorem 2.5 guarantees a permutation $\pi \in S_k$ such that $f(x_{\pi(i)}) + i$ are all distinct modulo $2n$. It follows that there exists a permutation $b_1, \ldots, b_k$ of L_i such that $f(x_j) + b_j$ are all distinct modulo $2n$. Define $f(y_j) = f(x_j) + b_j$, for $j = 1, \ldots, k$. It is clear that f now satisfies (a), (b) and (c) on the level sets $V_0, \ldots, V_i$ This completes the definition of f.

The desired embedding of T' can be described by defining $g : V(T') \to V(C_{4s}(2n))$ according to the rule $g(u) := (f(u), d_{T'}(u, v_1))$. Observe that property (c) and $4s \geqslant 2r + 1$ guarantee that g is one-to-one, property (a) implies that $g(v_1) = (0, 0)$, and property (b) implies that the labels on the edges connecting the vertices $\{g(u)\}_{u \in V_{i-1}}$ and $\{g(u)\}_{u \in V_i}$ are precisely the labels in L_i, for $i = 1, \ldots, 2r$, so all edges have distinct angles. □

The bounds in Theorem 3.1 can be improved by a multiplicative constant using an unpublished result of Häggkvist [6] that obviates the initial tree duplicating step of the proof.

Acknowledgement

The authors thank an anonymous referee for valuable suggestions that greatly improved the presentation of this paper.

References

[1] Alon, N. (1999) Combinatorial Nullstellensatz. *Combin. Probab. Comput.* **8** 7–29.
[2] Alon, N. (2000) Additive latin transversals. *Israel J. Math.* **117** 125–130.
[3] Alon, N. and Tarsi, M. (1992) Colorings and orientations of graphs. *Combinatorica* **12** 125–134.
[4] Hall, M. (1952) A combinatorial problem on abelian groups. *Proc. Amer. Math. Soc.* **3** 584–587.
[5] Hsu, F. (1980) *Cyclic Neofields and Combinatorial Designs*, Vol. 824 of *Lecture Notes in Mathematics*, Springer, Berlin/New York.
[6] Häggkvist, R. (1989) Decompositions of complete bipartite graphs. In *Surveys in Combinatorics*, Vol. 141 of *London Math. Soc. Lecture Note Ser.*, pp. 115–147.

[7] Ringel, G. (1964) Problem 25. In *Theory of Graphs and its Applications* (Proc. Symp. Smolence, 1963), Czech. Acad. Sci., p. 162.

[8] Rosa, A. (1967) On certain valuations of the vertices of a graph. In *Theory of Graphs* (Internat. Sympos. Rome, 1966), pp. 349–355.

[9] Snevily, H. (1997) New families of graphs that have α-labelings. *Discrete Math.* **170** 185–194.

[10] Snevily, H. (1999) The Cayley Addition Table of Z_n. *Amer. Math Monthly* **106** (6) 584–585.

[11] Snevily, H. (1997) A polynomial approach to the graceful tree conjecture. Manuscript.

[12] Yuster, R. (2000) Packing and decomposition of graphs with trees. *J. Combin. Theory Ser. B* **78** 123–140.

[13] Wilson, R. M. (1976) Decompositions of complete graphs into subgraphs isomorphic to a given graph. In *Proc. Fifth British Combinatorial Conference* (Univ. Aberdeen, Aberdeen, 1975), pp. 647–659. *Congressus Numerantium* **XV**, Utilitas Math., Winnipeg, Man.