REFERENCES

STUDENT RESEARCH PROJECTS

EDITOR

Brigitte Servatius
Department of Mathematical Sciences
Worcester Polytechnic Institute
Worcester, MA 01609-2280

From Cyclic Sums to Projective Planes

Roger Zarnowski (roger.zarnowski@angelo.edu), Angelo State University, San Angelo, TX 76909.

Sophisticated concepts often arise from casual observations. Here we present a property of ordered n-tuples that seems at first to be a mere curiosity. But it turns out that exploration of this property quickly leads to a wide variety of intriguing problems and to some important mathematical ideas.

Cyclic sum sets. We begin by considering the ordered triple of numbers $(1, 2, 4)$, although we treat the numbers as connected cyclically, like beads on a closed necklace. Consider the numbers that can be obtained by summing adjacent terms of this "necklace" in groups of lengths 1, 2, and 3. We call these *cyclic sums*. There are

3 cyclic sums of length 1 :		**1**
		2
		4
3 cyclic sums of length 2 :	$1+2=$	**3**
	$2+4=$	**6**
	$4+1=$	**5**
1 cyclic sum of length 3 :	$1+2+4=$	**7**

Interestingly, these seven cyclic sums are precisely the integers 1 through 7. Because of this very special property, we call $(1, 2, 4)$ a *cyclic sum set*. More generally, we make the following definition.

For an ordered set of positive integers $\mathbf{a} = (a_0, a_1, \ldots, a_n)$, a *cyclic sum* over $\mathbf{a}$ is an expression of the form $a_j + \cdots + a_{j+k}$, where $0 \le j, k \le n$ and all indices are computed modulo $n + 1$. The set $\mathbf{a}$ is called a *cyclic sum set* (CSS) of order n if the set of values of all cyclic sums over $\mathbf{a}$ is $\{1, 2, \ldots, N\}$, where N is the number of possible cyclic sums.

According to the definition, a CSS of order n has $n + 1$ terms. So, for example, $(1, 2, 4)$ is a CSS of order 2. Also, two CSSs are called the same if one can be obtained from the other by a cyclic permutation, a reversal of order, or a combination of these two.

Problem 1. Show that $N = n^2 + n + 1$ in the above definition, and that the sum of all terms in a CSS is also $n^2 + n + 1$.

Problem 2. Verify that (1) is the only CSS of order 0, $(1, 2)$ is the only CSS of order 1, and $(1, 2, 4)$ is the only CSS of order 2.

Problem 3. Show that a CSS of order greater than 0 must contain 1 and 2.

Several questions naturally come to mind. Does a CSS exist for every order n? Can there be more than one? Are there some interesting consequences of a set being a CSS? Solving the next problem should give a sense that there may not be easy answers to these questions.

Problem 4. Find all CSSs of orders 3 and 4.

The problem of finding CSSs becomes very difficult as n increases, and this suggests that a computer could be useful. We will discuss this further, but first we introduce some related ideas.

Cyclic difference sets. The set $\{1, 2, 4\}$ has another interesting property, this one involving differences instead of sums.

Problem 5. Show that the six differences of distinct terms of $\{1, 2, 4\}$ are congruent modulo 7 to the integers from 1 to 6.

Because of this property, the set $\{1, 2, 4\}$ is also an example of a *cyclic difference set* (see, for example, Baumert [**2**] or Ryser [**8**]). Much has been written about difference sets, and there are generalizations of the ones we consider here, but the following serves as an appropriate definition for our purposes.

A set of $n + 1$ integers $\{b_0, b_1, \ldots, b_n\}$ is a *cyclic difference set* (CDS) of order n if each integer $1, 2, \ldots, n^2 + n$ is congruent modulo $n^2 + n + 1$ to exactly one of the $n^2 + n$ differences $b_i - b_j$, for $i \neq j$.

Note that the order of terms is important for a CSS but not for a CDS, and so we use parentheses for the former and braces for the latter. Also, the addition or subtraction of a fixed number to each term of a CDS yields another CDS of the same order. To avoid this redundancy, we assume, unless specified otherwise, that CDSs are in "normal form", by which we mean in increasing order with 1 as the least term.

Problem 6. Show that the greatest term of a CSS is less than or equal to $\frac{n(n+1)}{2} + 1$.

Problem 7. Show that the greatest term of a CDS is greater than or equal to $\frac{n(n+1)}{2} + 1$.

Problem 8. Characterize those CSSs that are also CDSs.

Problem 9. Explore the relationship between CSSs and CDSs. For example, is there a one-to-one correspondence between the CSSs and the (normal form) CDSs of the same order?

Block designs and projective planes. Cyclic sum and difference sets are closely related to some other topics, which we now explore. Consider a CDS $\{b_0, b_1, \ldots, b_n\}$ in normal form. With $N = n^2 + n + 1$, generate a collection of N difference sets of the form

$$\{(b_0 + j) \bmod N, (b_1 + j) \bmod N, \ldots, (b_n + j) \bmod N\},$$

where j ranges from 0 to $N - 1$. We now refer to each CDS as a "block" and number the blocks 1 through N, so that the first block corresponds to $j = 0$ and block N to

$j = N - 1$. For example, with our familiar CDS (1, 2, 4), since $n = 2$, we obtain the blocks

$$\{(1, 2, 4), (2, 3, 5), (3, 4, 6), (4, 5, 0), (5, 6, 1), (6, 0, 2), (0, 1, 3)\}.$$

This is a particular example of a *block design*. By considering the numbers 0-6 as points on a circle, with a triangle connecting the numbers 1, 2, and 4, these blocks may be thought of as being generated by rotating the triangle around the circle, as illustrated in Figure 1. Block designs have many important applications in cryptography and statistics. More general forms are discussed in Brualdi [**4**] and Ryser [**8**].

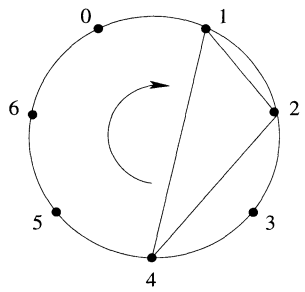

Figure 1. Generation of a Block Design.

The block design in our example also has the following remarkable properties: each pair of numbers appears in exactly one of the seven blocks, and each pair of blocks has exactly one number in common. It turns out that these properties generalize.

Problem 10. Consider the $n^2 + n + 1$ blocks obtained from a CDS of order n by the process outlined above. Prove that each pair of numbers from the set $\{0, 1, \ldots, n^2 + n\}$ appears in exactly one block, and that each pair of blocks has exactly one number in common.

This result has a wonderful geometric interpretation. A *projective plane* is a geometry defined in terms of "points" and "lines" with the property that any two points are incident with exactly one line, and any two lines are incident with exactly one point (see, for example, Polster [**7**] or Beutelspacher and Rosenbaum [**3**]). A finite projective plane of order n has $n^2 + n + 1$ points and the same number of lines. It also has the property that each line contains exactly $n + 1$ points and each point lies on exactly $n + 1$ lines. Our example is a projective plane of order 2 with seven points and seven lines (the seven blocks). This is known as the Fano plane, a standard representation of which is shown in Figure 2. The "lines" in the Fano plane appear in the figure as six ordinary line segments and a circle. The Fano plane, and other projective planes that are associated with cyclically generated block designs, are called *cyclic planes*.

Problem 11. Sketch a representation of a finite projective plane of order 3.

Difference sets, block designs, and projective planes have some surprising applications, such as in the design of efficient communications networks (Parhami [**6**]). Also, it is known that a cyclic projective plane exists whenever the order n is a power of a prime number, and when the order is prime the cyclic plane is the only one known. No

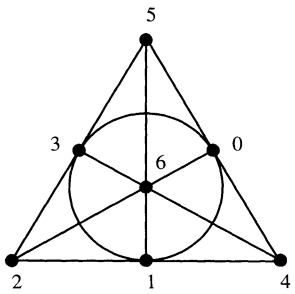

Figure 2. The Fano plane.

projective planes are known for other orders. A famous open problem is to prove or disprove the Prime Power Conjecture, which asserts that finite projective planes exist only for prime power orders.

The following problem is a natural one to investigate at this point, although it is open-ended and possibly difficult to answer unambiguously.

Problem 12. Investigate relationships between CSSs of a particular order and cyclic projective planes of the same order.

Computing projects. We now return to the problem of finding all CSSs of a given order n, which we refer to simply as "the CSS problem". In attempting to do this by hand, one soon discovers that the problem becomes enormously difficult as n increases. It seems natural to write a computer program for the task, and this effort leads not only to some interesting computational challenges but also to another intriguing mathematical concept, that of integer partitions.

A partition of a positive integer N is simply a set of positive integers whose sum is N, without regard to order. For example, $\{1, 1, 1\}$, $\{1, 2\}$, and $\{3\}$ are the partitions of 3. The theory of integer partitions is itself a fascinating topic in number theory, and one with a rich history. Andrews [1] provides an excellent introduction. For our purposes it suffices to note that a CSS of order $n > 1$ is a partition of $n^2 + n + 1$ that contains the numbers 1 and 2 (by Problem 4). We can use this fact to address the CSS problem computationally in the following three steps.

Problem 13. Given an integer $n \geq 1$, write a program to find all partitions of $n^2 + n + 1$ into $n + 1$ distinct parts, including the numbers 1 and 2. (Although relatively straightforward, this is an important preliminary step in generating candidates for CSSs.)

Problem 14. Given a partition $\{a_1, a_2, \ldots, a_n\}$ of $n^2 + n$ (using the results of the previous program, and considering $a_0 = 1$ fixed), write a program to generate all permutations of this set. This is precisely the problem of generating all $n!$ permutations of n objects, but efficiency is extremely important here; sophisticated algorithms are easy to find and well worth investigating.

Problem 15. Write a program to test an $(n + 1)$-tuple $(a_0, a_1, \ldots, a_n)$ for the CSS property.

The CSS problem becomes very difficult as n increases, and it is often of great interest to quantitatively describe such complexity. We can do so by using the results of

a program such as the one outlined above. First consider a more rudimentary algorithm, one in which each term of an n-tuple is iterated from 1 to a maximum value M, which depends on n. The number of possible n-tuples is then M^n. If we assume that M varies as a power of n, then it is reasonable to represent the CPU time T_n by a function of the form $T_n = Cn^{kn}$ for some constants C and k. This form is general enough to also be reasonably applied to the algorithm outlined in Problems 13–15. Then

$$\frac{T_{n+1}}{T_n} = \left[\frac{(n+1)^{n+1}}{n^n}\right]^k,$$

so that

$$k = \frac{\log\left[T_{n+1}/T_n\right]}{\log\left[(n+1)^{n+1}/n^n\right]}.$$

Most programming languages have a means for measuring the CPU time required to execute a program. If the last expression is approximately constant for different values of n, then we have strong reason to accept the assumed functional form for T_n, and we can use our data to approximate k and C.

Problem 16. Record the CPU times required to solve the CSS problem until you reach a value of n for which you are no longer willing to wait on your computer. Use the data to approximate C and k, and compare values of Cn^{kn} with the actual CPU times. Then estimate the time required to complete the search for the next value of n.

The results of these computations may give insight into some of the preceding problems. They should also give an appreciation for just how quickly the CSS problem becomes intractable, even with modern computers. Lam [**5**] relates the fascinating history of how computers were used over a period of many years to confirm that there is no projective plane (cyclic or noncyclic) of order 10, as asserted by the Prime Power Conjecture.

References

1. G. E. Andrews and K. Eriksson, *Integer Partitions*, Cambridge Univ. Press, 2004.
2. L. D. Baumert, *Cyclic Difference Sets*, Springer-Verlag, 1971.
3. A. Beutelspacher and U. Rosenbaum, *Projective Geometry*, Cambridge Univ. Press, 1998.
4. R. A. Brualdi, *Introductory Combinatorics*, Prentice-Hall, 1992.
5. C. W. H. Lam, The Search for a Finite Projective Plane of Order 10, *Amer. Math. Monthly*, **98** (1991) 305–318. (Also available online at `http://www.cecm.sfu.ca/organics/papers/lam/`.)
6. B. Parhami and M. Rakov, Application of Perfect Difference Sets to the Design of Efficient and Robust Interconnection Networks, *Proc. 2005 International Conf. on Communications in Computing*, CSREA Press, 2005, 207–216.
7. B. Polster, *A Geometrical Picture Book*, Springer, 1998.
8. H. J. Ryser, *Combinatorial Mathematics*, MAA, 1963.