Higher Dimensional Periodic Sequences

Recall that a sequence $s_0, s_1, s_2, \ldots$ of elements of the finite field $\mathbb{F}_q$ with q elements is called a k[th] order homogeneous linear recursive sequence if it satisfies a relation of the form $s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \cdots + a_0 s_n$ for all $n = 0,1,2,\ldots$, where $a_0, \ldots, a_{k-1}$ are fixed elements of $\mathbb{F}_q$. Any such relation for the sequence gives rise to a polynomial $f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_0 \in \mathbb{F}_q[x]$ called a characteristic polynomial of the sequence. There exists a uniquely determined characteristic polynomial $m(x)$ of minimal degree, called the minimal polynomial of the sequence.

The structure and properties of homogeneous linear recursive sequences have been extensively studied (for a general reference, see [2]). Applications of these sequences abound. For example, they are used in linear feedback shift registers, in generating certain classes of error correcting codes, and stream ciphers in cryptography. One particular property of interest is the period (that is, the smallest number r such that $s_{n+r} = s_n$ for all $n \geq n_0$ for some integer $n_0 \geq 0$) of a homogeneous linear recursive sequence. It is well known that the period is equal to the order of the polynomial $m(x)$, that is, the least positive integer *e* such that $m(x) \mid x^e - 1$ in $\mathbb{F}_q[x]$.

An *n*-dimensional sequence over the finite field $\mathbb{F}_q$ is a function $s : \mathbb{N}^n \to \mathbb{F}_q$. An *n*-dimensional sequence s is called a linear recursive sequence if it is annihilated by a zero dimensional ideal of the ring $\mathbb{F}_q[x_1, \ldots, x_n]$. However, it is equivalent to saying that, for each k, there is a polynomial $m_k(x_k) \in \mathbb{F}_q[x_k]$ in the indeterminant x_k such that for each choice of nonnegative integers $i_1, \ldots, i_{k-1}, i_{k+1}, \ldots, i_n$, the one-dimensional sequence $s(i_1, \ldots, i_{k-1}, 0, i_{k+1}, \ldots, i_n), s(i_1, \ldots, i_{k-1}, 1, i_{k+1}, \ldots, i_n), s(i_1, \ldots, i_{k-1}, 2, i_{k+1}, \ldots, i_n), \ldots$ has characteristic polynomial $m_k(x_k)$. The polynomials $m_k(x_k)$ are useful in determining various properties of the *n*-dimensional sequence *s*. For example, in [1] the irreducible factors of the polynomials $m_k(x_k)$ were used to find the size of a generating set of all sequences having the same annihilating ideal. In the two-dimensional case the linear recursive sequences are sometimes called linear recurring arrays. The periods of such arrays have been investigated quite extensively (see, e.g., [3]).

The author proposes investigating these polynomials further. In particular, as a first level of research, the students will investigate whether there is an analogous statement relating the size of a period window of an *n*-dimensional linear recursive sequence to that of the orders of the polynomials $m_k(x_k)$. Computer programs such as *Mathematica* can be used to generate data to be used to formulate conjectures about the relationship between the period window and the orders of the polynomials $m_k(x_k)$. For a second level of research, students can investigate *n*-dimensional linear recursive sequences over Galois rings (or, more generally, artinian rings such as in [4]), and the size of a period window of such sequences. The introduction of nilpotent elements may complicate the relationship of the period to that of the orders of the polynomials $m_k(x_k)$, providing fertile ground for more investigation. At a third level of research, students can

investigate the distribution of elements in such sequences. Using computer generated data, students will try to establish estimates concerning the number of occurrences of elements in such sequences.

The connection to some elementary topics in discrete mathematics, such as Fibonacci sequences, modular arithmetic, and solving recurrence relations, and the ability to generate lots of data with a computer, will make this topic readily accessible to undergraduates. In the course of this project, students can be expected to gain knowledge of the algebraic underpinnings of *n*-dimensional linear recursive sequences. In particular, students will come away with a greater understanding of finite fields and rings, and polynomials rings over finite fields. Since these topics of mathematics provide some of the foundations in other areas of mathematics, such as algebraic coding theory, this project should be quite attractive to undergraduates with an interest in the burgeoning field of communication theory. This project can also be a springboard for the students to pursue further research in these areas in graduate school and beyond.

Prerequisites: One semester of discrete mathematics and one semester of abstract algebra.

References

[1] Fu, D., Heiligman, M., and Wickham, C., *Decomposition of tableaus annihilated by zero dimensional ideals*, J. Algebra, **267** (2003), no. 2, 404--420.

[2] Lidl, R. and Niederreiter, H, Introduction to finite fields and their applications, Cambridge University Press, Cambridge, 1986.

[3] Sakata, S., *General theory of doubly periodic arrays over an arbitrary finite field and its applications*, IEEE Trans. Inform. Theory **24** (1978), no. 6, 719--730.

[4] Wickham, C., *Decomposition of n-dimensional recursive sequences over finite rings*, preprint, (2003).