OCCIDENTAL COLLEGE REU 2023: POTENTIAL PROBLEMS

A. **Potential Research Problems.**

Some possible problems for this summer are outlined below in Sections A-1 and A-2. This list is by no means exhaustive of the problems under consideration, it merely provides a representative sample of the types of problems under consideration. Students will have some say in picking the problems so they can work on something of interest.

A-1. **Arithmetic structures on graphs.** Let G be a connected non-oriented graph with n vertices $V_1, \ldots, V_n$. Let c_{ij} be the number of edges linking V_i to V_j. Let A denote the adjacency matrix of G, i.e., $A = (a_{ij})$ with $a_{ii} = 0$ and $a_{ij} = c_{ij}$ for $i \neq j$.

Definition A.1. *An arithmetical graph consists of a connected graph G, a diagonal matrix $D = \operatorname{diag}(d_1, \ldots, d_n)$ with $d_i \in \mathbf{Z}_{\geq 1}$, and a vector $R = (r_1, \ldots, r_n)$ with $r_i \in \mathbf{Z}_{\geq 1}$ and $\gcd(r_1, \ldots, r_n) = 1$ so that $(D - A)R = 0$; we denote this by (G, M, R) where $M = D - A$.*

One should note that each connected graph has an least one arithmetical structure on it, namely, set d_i to be the degree of the vertex V_i.

The matrices M arise in algebraic geometry, in particular, they are intersection matrices of degenerating curves [4]. There has been work on arithmetical graphs purely from the graph theoretic point of view, and that is what is proposed here. For instance, it is shown in [4] that there are a finite number of arithmetical structures on any particular graph [4, Lemma 1.6]. If one restricts to considering paths and cycles one can get more precise results. For instance, the number of arithmetical structures on the path $\mathcal{P}_n$ is the Catalan number $C_{n-1} = \frac{1}{n}\binom{2n-2}{n-1}$ [1, Theorem 3].

While requiring D and R to have integer entries is natural when considering this from an algebraic geometry point of view, it is interesting to extend the notion of an arithmetical structure on a graph to include other arithmetic rings. For instance, instead of requiring D and R to have integer entries, one could consider D, R to have entries consisting of monic polynomials in $\mathbf{F}_p[T]$. As is well known, the ring $\mathbf{F}_p[T]$ mimics many of the interesting arithmetic properties of $\mathbf{Z}$ and requiring the polynomials to be monic is a natural replacement for requiring $d_i, r_i \in \mathbf{Z}_{\geq 1}$. It would also be interesting to consider rings of integers of number fields, $\mathbf{Z}[i]$ or $\mathbf{Z}[\sqrt{3}]$ for example. When we replace $\mathbf{Z}_{\geq 1}$ with a ring $\mathcal{O}$, we will refer to this as an $\mathcal{O}$-arithmetical structure.

Project 1 The first step in such generalizations is to gather examples and computational data. The students will learn about $\mathbf{F}_p$, how to compute in the ring $\mathbf{F}_p[T]$, and work out examples of $\mathbf{F}_p[T]$-arithmetic structures on various graphs. Ideally they will classify all $\mathbf{F}_p[T]$-arithmetic structures on some basic graphs like short paths.

Project 2 This project would either go after Project 1 if the REU students moved particularly fast, or it could be an REU project for a future summer after students have worked on the first project and produced results that can be read by the future students. The project will be to investigate the following questions. Are there finitely $\mathbf{F}_p[T]$-arithmetical structures on a connected non-oriented graph G? How about if we consider other rings such as the ring of integers in a number field? For a totally real number field it would be natural to consider elements that are totally positive, i.e., they are positive for all real embeddings of the field. For number fields that are not totally real, it may be most natural to work with ideals to avoid the issue of positivity of the elements. Some of these ideas would require some abstract algebra, but particular cases could be worked out without a great deal of required background; the particular abstract algebra needed would be taught in the first 2-3 weeks of the program.

Project 3 In addition to the general questions in the previous project, we can examine $\mathcal{O}$-arithmetical structures on simple graphs such as paths and cycles. This is done for $\mathcal{O} = \mathbf{Z}$ in [1]. It will be interesting to see how the count changes when one replaces $\mathbf{Z}$ with other interesting rings. For instance, is the arithmetic of the ring $\mathcal{O}$ reflected in the counts and if so, how?

A-2. **Coding theory, lattices, and theta series.** Let p be a prime and consider a finite field $\mathbf{F}$ of cardinality $q = p^f$ for some $f \geq 1$. A $[n,k]$-linear code $\mathcal{C}$ is a k-dimensional subspace of the vector space $\mathbf{F}^n$. We refer to elements of $\mathcal{C}$ as codewords. Binary codes, i.e., codes where $p = 2$, are well-studied (at least for $f = 1, 2$), but codes for $p > 2$ or for $f > 2$ are less prevalent in the literature. For simplicity, consider an $[n,k]$-code $\mathcal{C}$ defined over $\mathbf{F}_p$. One has a natural surjective map $\pi : \mathbf{Z}^n \to \mathbf{F}_p^n$ given by reduction modulo p in each component. Using this surjection, one has a lattice $\pi^{-1}(\mathcal{C}) = \Lambda_{\mathcal{C}} \subset \mathbf{Z}^n$ associated to $\mathcal{C}$ and this lattice reflects some of the properties of the code. For instance, $\mathcal{C}$ is self-dual if and only if $\Lambda_{\mathcal{C}}$ is unimodular. In the case $f > 1$, there is not a canonical surjection from $\mathbf{Z}^n$ onto $\mathbf{F}^n$, but one can construct a surjection $\pi : \mathcal{O}^n \to \mathbf{F}^n$ where $\mathcal{O}$ is the ring of integers of a number field where p has the appropriate factorization so that $\mathbf{F}$ can be realized as a quotient of $\mathcal{O}$. During the summer of 2018 the PI co-supervised a group of students with F. Manganiello that studied codes and their related lattices and theta series for $f = 2$. In particular, they showed that one can construct a field $K = \mathbf{Q}(\sqrt{d})$ with p inert in K and a field $L = K(\zeta_p)$ so that one has a surjection $\mathcal{O}_L^n \to \mathbf{F}^n$. Moreover, they showed that under this construction the lattice arising from a self-dual code $\mathcal{C}$ is not a unimodular lattice. Associated to the lattice $\Lambda_{\mathcal{C}}$ they constructed a theta series $\theta_{\mathcal{C}}$ that is a Hilbert modular form. During the summer of 2021 the PI supervised a group of four students that considered real quadratic fields $K = \mathbf{Q}(\sqrt{\ell})$ so that 2 is inert in $\mathcal{O}_K$ which gives a surjection $\mathcal{O}_K^n \to \mathbf{F}_4^n$ given by reduction modulo 2. The students studied the theta series as one varies ℓ. They showed that if one fixes a code $\mathcal{C}$, the theta series for various ℓ agree up to a certain number of coefficients. While the theta series are modular forms, that fact was used in the project of 2018 but not at all in 2021 so one can vary the level of difficulty of these projects based on the student's background. Some further projects in this area:

Project 1 It is known from the work of the 2021 REU group that if one considers real quadratic fields $K_1 = \mathbf{Q}(\sqrt{\ell_1}), K_2 = \mathbf{Q}(\sqrt{\ell_2})$ where 2 is inert in K_1, K_2, then the theta series $\theta_{\mathcal{C},\ell_1}$ and $\theta_{\mathcal{C},\ell_2}$ associated to a code $\mathcal{C}$ have a certain number of equal Fourier coefficients with the number depending on the smaller prime ℓ_1, ℓ_2. A similar result is known for imaginary quadratic fields ([2, 3, 6].) The next natural step is to consider fields that are not quadratic. For instance, one can consider cubic fields with abelian Galois group. One can show that one can construct a surjection, lattice, and theta series as in the quadratic case here as well. While one does not have an easy way to vary the fields in an infinite family as in the quadratic case, one can still look at the theta series and see if they agree as one changes fields. This could be done for codes over $\mathbf{F}_8$ or $\mathbf{F}_{p^3}$. One could also play this same game with other fields such as $\mathbf{Q}(\zeta_p)$ for codes over $\mathbf{F}_p$ or more generally over $\mathbf{Q}(\zeta_n)$ for other finite fields $\mathbf{F}$ depending on how p factors in $\mathbf{Q}(\zeta_n)$. This area of inquiry allows students to learn algebra and some number theory while exploring tractable problems along these lines. This area is full of undergraduate level problems to explore.

Project 2 In the REU project from 2018 a relation between the theta series $\theta_{\mathcal{C}}$ and the complete weight enumerator of the code was given. However, this was not optimal as it did not take into account all of the symmetries of the theta series. One would like to construct an appropriate generalized Lee weight as defined in [5] so that the theta series is given in terms of this weight. This involves finding a map from $\mathbf{Z}^{nj} \to \mathbf{F}_{p^2}^n$ for some $j \geq 1$

that captures the symmetries of the theta series when one calculates the weights of the codewords. Experimenting with various such weight functions is an interesting project. One could also computationally look for relations between the theta series associated to the code and various weight one theta series and try to reverse engineer the generalized Lee weight from the relations found. Again, this sounds very complicated but it can be done with a computer algebra system as it essentially comes down to calculating some Fourier coefficients and then looking at monomials relations between the series.

References

[1] B. Braun, H. Corrales, S. Corry, L. D. García Puente, D. Glass, N. Kaplan, J. Martin, G. Musiker, and C. Valencia. Counting arithmetical structures on paths and cycles. *Discrete Math.*, 341(10):2949–2963, 2018.

[2] K. Chua. Codes over GF(4) and $\mathbf{F}_2 \times \mathbf{F}_2$ and Hermitian lattices over imaginary quadratic fields. *Proc. Amer. Math. Soc.*, 133(3):661–670, 2005.

[3] K. Chua. Codes over GF(4) and $\mathbf{F}_2 \times \mathbf{F}_2$ and Hermitian lattices over imaginary quadratic fields. *Proc. Amer. Math. Soc.*, 133(3):661–670, 2005.

[4] D. Lorenzini. Arithmetical graphs. *Math. Ann.*, 285(3):481–501, 1989.

[5] S. Nishimura and T. Hiramatsu. A generalization of the Lee distance and error correcting codes. *Discrete Appl. Math.*, 156(5):588–595, 2008.

[6] T. Shaska and G. S. Wijesiri. Codes over rings of size four, Hermitian lattices, and corresponding theta functions. *Proc. Amer. Math. Soc.*, 136(3):849–857, 2008.