Comments on dissertations

John Moseley, “Some representations of unitary groups” (1974).

In the paper “Representations of symplectic groups” [*J. Algebra* **20** 1972 182–195] I rediscovered the Weil representation (unknown to me!), constructing it by using a twisted group algebra built on a symplectic space. Let V be a $2n$-dimensional vector space over $\mathbb{F}_q$, q a power of the odd prime p, endowed with a nondegenerate symplectic form φ. Let R be an integral domain of characteristic not equal to p, and let ε be a primitive p-th root of unity in R. Make the free R-module $\mathcal{A}$ with basis the symbols (x), $x \in V$, into a a twisted group algebra for the additive group of V by defining $(x)(y) = \varepsilon^{\mathrm{trace}(\varphi(x,y))}(x+y)$; the trace is from $\mathbb{F}_q$ to $\mathbb{F}_p$. Then a determinant argument shows that $\mathcal{A}$ is nothing more than $q^n \times q^n$ matrix algebra over R. If g is a semilinear transformation preserving φ, then the map $(x) \to (x^g)$ defines an automorphism of $\mathcal{A}$. By the Skolem-Noether theorem this automorphism is inner; thus one gets a representation of degree q^n of $\Gamma\mathrm{Sp}(V)$, the group of these semilinear transformations (of which the symplectic group $\mathrm{Sp}(V)$ is a subgroup). If $\mathrm{char}(R) \neq 2$, the representation has two composition factors of degrees $(q^n \pm 1)/2$, and if $\mathrm{char}(R) = 2$, one factor of degree $(q^n - 1)/2$ appearing twice, with the trivial representation in between. The irreducible representations can be written in rather small fields.

I suspected that there were analogous results for unitary groups in place of symplectic groups. John verified this suspicion in great detail. Finding the irreducible constituents of the initial matrix representation was a major problem that John solved very thoroughly. He investigated natural invariant forms on the representation spaces and the fields in which the representations could be written.

Don Newhart, “Information sets in quadratic-residue codes” (1977).

The Weil representation can be used to give a presentation of (generalized) quadratic residue codes [“Quadratic residue codes and symplectic groups,” *J. Algebra* **29** (1974), 150–171], and this discovery was really my first work in coding theory. In effect, the Gleason-Prange theorem is built into the definition this way, a fact surely known to Gleason. In this framework, there are two natural coordinate subsets that might serve as information sets, and Don examined these possibilities. His work entailed investigating actions of the special linear group, and he sought help from Leonard Scott. Don became interested in the question of the minimum weight of quadratic residue codes and he developed sophisticated methods for determining that minimum weight by computer searches. This led to the paper “On minimum weight codewords in QR codes” [*J. Combin. Theory Ser. A* **48** (1988), no. 1, 104–119].

Don’s thesis was published as “Information sets in quadratic-residue codes” [*Discrete Math.* **42** (1982), no. 2-3, 251–266].

Jim Davis, "Difference sets in Abelian 2-groups" (1987).

Jim has become an expert on difference sets, and I recommend exploring his publications through MathSciNet.

Julia Morrisett Clark, "Relations between quadratic residue codes written in their defining field and certain other classical codes" (1991).

Julia's work also dealt with quadratic residue codes. From the Weil representation approach, there is a rather natural definition of spanning sets for quadratic residue codes. One starts with the assumption that the characteristic of the field in which the codes are written is different from that of the field of the underlying symplectic group. But on reworking this set, one finds that this assumption can be dropped; new codes are produced that still allow an action of $\Gamma\mathrm{L}(2, q)$ as for the standard codes, and I wrote on this in "Quadratic residue codes in their prime" [*J. Algebra* **150** (1992), no. 1, 87–100]. These codes are in effect the modular constituents of the standard codes. Julia dealt with questions of minimum weight and the relation of these codes to Reed-Muller codes.

Jim Wilmot: "Topics in divisible codes" (1994).

A linear code is called *divisible*, with divisor $\Delta > 1$, if all the word weights of the code are multiples of Δ. It is natural to look for bounds on the code dimension in terms of the combination of minimum weight and divisor. Jim investigated binary codes for which the divisor and minimum weight were both the same power of 2, relating codes meeting his bound to Reed-Muller codes.

Jim also investigated the then recently classified (32,16) extremal type II binary codes, searching for instances of these codes that contained highly divisible subcodes.

Deirdre Smeltzer, "Topics in difference sets in 2-groups" (1994).

Reed-Muller codes have been related to ideals in group algebras by several mathematicians. In the paper "Divisors of codes of Reed-Muller type" [*Discrete Math.* **131** (1994), no. 1-3, 311–323] I investigated divisibility properties of codes that are generalizations of the powers of the radical of the group algebra of a p-group over a field of characteristic p, p a prime. Deirdre applied these ideas to codes obtained from difference sets in 2-groups, studying divisibility properties of the code of a difference set and subcodes obtained by multiplying by the radical. She also obtained results on bent functions.

Deirdre's work appeared in "Properties of codes from difference sets in 2-groups" [*Des. Codes Cryptogr.* **16** (1999), no. 3, 291–306].

Todd Vance, "Missing weights in GRM codes" (1997).

Generalized Reed-Muller (GRM) codes from an important class of codes with many connections to geometry and properties of polynomials. By and large, they are divisible codes, the divisor being determined by the parameters. Their weight distributions are pretty much unknown. If the divisor is Δ, the weights in such a code will begin at the minimum weight d and increase by multiples of Δ; but the weights may not appear as consecutive multiples of Δ; there may be “gaps.” For binary GRM codes (the classical Reed-Muller codes), the exact weights are known for first and second order codes (and their duals, which are also Reed-Muller codes), and gaps appear. Todd developed intricate methods for finding gaps in the case of ternary ($p = 3$) GRM codes, looking in particular for when the next multiple $d + \Delta$ was not present as a code-word weight.

Todd published his work in “A gap in GRM code weight distributions” [*Des. Codes Cryptogr.* **19** (2000), no. 1, 27–43].

Kevin Chouinard, “Weight distributions of codes from finite planes” (1998).

Kevin worked jointly with Gary McGuire and me; Gary was a post-doc at Virginia. Gary and I had just completed the determination of the weight enumerator of the code of the projective plane of order 5, by hand–it was later verified by Jenny Key, using MAGMA (“A determination of the weight enumerator of the code of the projective plane of order 5”, *Note Mat.* **18** (1998), no. 1, 71–99 (1999)). The codewords of small weight were especially interesting, being related to various geometric configurations. In particular, there are conspicuous gaps in the weights (the codes are not divisible). Kevin searched for analogous gaps in the codes for other planes, proving some general results and then analyzing the plane of order 8 in some detail. He also sought to discover what configurations arose in connection with the words. His work has continued to spark interest in such questions; it fits in well with investigations by Jenny Key and her students.

Kevin’s thesis appears as “On weight distributions of codes of planes of order 9” [*Ars Combin.* **63** (2002), 3–13].

John Polhill, “Constructing difference sets and partial difference sets using Galois rings” (1999).

John did his work jointly with Jim Davis and me. Continuing with a project that John worked on with Jim at the University of Richmond, John generalized constructions for partial difference sets due to Jim and to K. H. Leung and S. L. Ma, obtaining three families of such sets in the group $(\mathbf{Z}_{p^r})^{2t}$ for $r \geq 2$. His constructions were actually carried out in the context of Galois rings.

John’s work was published as “Constructions of nested partial difference sets with Galois rings” [*Des. Codes Cryptogr.* **25** (2002), no. 3, 299–309].

Chris Boner, “Characterization of absolute summands of categories of divisible codes” (1999).

Chris’s work was inspired by a paper of Ed Assmus on categories of codes [“The category of linear codes,” IEEE Trans. Inform. Theory 44 (1998), no. 2, 612–629)]. He sought to put divisible codes into such a category framework, seeking to characterize the indecomposable divisible codes. One resource he invoked was a paper of mine giving a computational method for determining the divisor of a code in terms of a spanning set for the code ["Weight polarization and divisibility," *Discrete Math.* **83** (1990), no. 2-3, 315–326]. Apart from my use of this paper in dealing with codes of Reed-Muller type, upon which Deirdre drew, this was the first in-depth use of the results of that paper. And I think Ed was pleased to know that Chris was working with his category approach to codes.

Chris also studied projective generalized Reed-Muller codes in his thesis, and this work was published as "Maximal weight divisors of projective Reed-Muller codes" [*Des. Codes Cryptogr.* **24** (2001), no. 1, 43–47].

Leslie Hatfield, "Words of small weight in the dual codes of projective planes of orders 9 and 25" (2003).

Leslie's work started under the guidance of Kelle Clark, a post-doc at Virginia who had been a student of Jenny Key. As her title suggests, her investigations continued in the vein of the research by Gary McGuire, Kevin Choiunard, and me. Once again, the problem dealt with describing words in codes of projective planes (or the dual codes) in terms of geometric configurations. Leslie dealt with all the planes of orders 9 and 25, not just the Desaruesian ones. Thus coordinate methods were not available; the arguments are much more combinatorial. however, she considered translation planes in some depth, where the group structure helps in the analysis.

Leslie was a coauthor with Kelle, Jenny Key, and me on a paper that incorporated some of her work: "Dual codes of projective planes of order 25" [*Adv. Geom.* 2003, suppl., S140–S152].