C.R. Math. Rep. Acad. Sci. Canada

Vol. X, No. 5 October 1988 octobre

CONTENTS

ISSN 0706-1994
Second class mail Registration 5324

On the Periods of Modular Elliptic Curves

Glenn Stevens

Presented by G. de B. Robinson, F.R.S.C.

Abstract: This is a survey of the results of [5]. Let $\mathcal{A}$ be a Q-isogeny class of elliptic curves. In §1 we define a partial ordering on $\mathcal{A}$ and prove that $\mathcal{A}$ has the greatest lower bound property. The minimal curve A_{min} is determined (uniquely) by the condition that its Neron lattice $\mathcal{L}(A_{min})$ is contained in the Neron lattice of every other curve in $\mathcal{A}$. In §2 we assume that $\mathcal{A}$ is modular with associated weight two newform f and define another lattice $\mathcal{L}(f)$ in the complex plane. We conjecture that the lattices $\mathcal{L}(A_{min})$ and $\mathcal{L}(f)$ are identical. The known evidence for this conjecture is summarised in Theorem 3.1.

§1 The Minimal Lattice of an Isogeny Class.

Let $A_{/\mathbf{Q}}$ be an elliptic curve defined over Q and let $\pm\omega_A$ be the Neron differentials on A. The complex points $A_{\mathbf{C}}$ of A define a compact Riemann surface of genus 1 on which ω_A defines a holomorphic 1-form. The periods obtained by integrating ω_A over 1-cycles on $A_{\mathbf{C}}$ form a lattice $\mathcal{L}(A)$ in the complex plane which we call the *Neron lattice*.

$$\mathcal{L}(A) \stackrel{def}{=} \text{Image}\left(H_1(A_{\mathbf{C}};\mathbf{Z}) \xrightarrow{\int \omega_A} \mathbf{C}\right) \tag{1.1}$$

Two elliptic curves A, B are Q-isomorphic if and only if $\mathcal{L}(A) = \mathcal{L}(B)$. They are Q-isogenous if and only if their lattices are commensurable: $\mathcal{L}(A) \otimes \mathbf{Q} = \mathcal{L}(B) \otimes \mathbf{Q}$.

Let $\mathcal{A}$ be a Q-isogeny class of elliptic curves. Then the Neron lattices of the curves in $\mathcal{A}$ form a finite collection of pairwise commensurable lattices in the complex plane. These lattices are partially ordered by inclusion. We can therefore define a partial ordering on $\mathcal{A}$ by $A \prec B \Leftrightarrow \mathcal{L}(A) \subseteq \mathcal{L}(B)$ for $A, B \in \mathcal{A}$.

(1.2) Theorem. *Let $\mathcal{A}$ be a Q-isogeny class of elliptic curves. Then the set of Neron lattices for $\mathcal{A}$ is closed under intersections: for each pair of curves $A, B \in \mathcal{A}$ there is a curve $C \in \mathcal{A}$ such that $\mathcal{L}(A) \cap \mathcal{L}(B) = \mathcal{L}(C)$. Thus every non-empty subset of $\mathcal{A}$ has a greatest lower bound.*

In particular, there is a unique curve $A_{min} \in \mathcal{A}$ for which

$$\mathcal{L}(A_{min}) = \bigcap_{A \in \mathcal{A}} \mathcal{L}(A).$$

We refer to A_{min} as the *minimal curve* and to $\mathcal{L}(A_{min})$ as the *minimal lattice* of the isogeny class $\mathcal{A}$.

The ordering $\prec$ can also be defined in terms of arithmetic properties of the isogenies in $\mathcal{A}$.

(1.3) Proposition. *Let ω_A, ω_B be Neron differentials on $A, B \in \mathcal{A}$. The following are equivalent:*

(a) $A \prec B$;

(b) There is a Q-isogeny $\phi : A \to B$ such that $\phi^*\omega_B = \pm\omega_A$;

(c) There is a Q-isogeny $\phi : A \to B$ whose extension to Neron models over Z is an étale morphism. ∎

A Q-isogeny $\phi : A \to B$ will be called an *étale isogeny* if either of the equivalent conditions (b) or (c) is satisfied. Étale isogenies are necessarily cyclic. Conversely, if $A \prec B$ and $\phi : A \to B$ is a cyclic isogeny then ϕ is étale.

(1.4) **Remark.** The *Parshin-Faltings height* of an elliptic curve $A_{/\mathbf{Q}}$ with Neron differential ω_A is defined to be

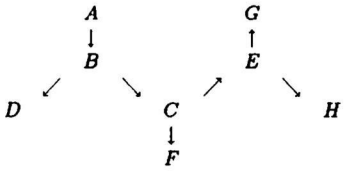
$$H(A) = \frac{1}{\sqrt{\text{covolume}(\mathcal{L}(A))}} = \left(\frac{1}{2\pi i}\int_{A_{\mathbf{C}}} \omega_A \wedge \overline{\omega}_A\right)^{-1/2}.$$

For two curves $A, B \in \mathcal{A}$ we clearly have the implication $A \prec B \Rightarrow H(A) \leq H(B)$. Thus A_{min} is also characterized as the unique curve of minimal height in $\mathcal{A}$. Since the Parshin-Falting's height roughly approximates the naive height of an elliptic curve, we expect the ordering of $\mathcal{A}$ to roughly reflect the size of the coefficients in the minimal Weierstrass equations of the curves in $\mathcal{A}$. This heuristic is easy to check against the Antwerp tables [6]. These tables present the coefficients of minimal Weierstrass equations for 749 elliptic curves over Q which are partitioned into 281 Q-isogeny classes. Our heuristic suggests that for each isogeny class $\mathcal{A}$, A_{min} should be the first curve found by the search methods employed in constructing the Antwerp tables, and should therefore be the first curve listed. I have used Gauss's AGM algorithm [2] to compute the Neron lattice of each curve in the Antwerp tables and have found that this expectation is correct for all but 7 isogeny classes. The complete list of minimal curves which appear in the Antwerp tables but are *not* listed first in their respective isogeny classes is:

89B, 98B, 128H, 130J, 141G, 150G, 168B.

For each isogeny class in the Antwerp tables a graph is provided which indicates all cyclic isogenies within that class. Once the minimal curve is known it is a simple matter using (1.6)(a) to replace this graph by the directed graph of étale isogenies.

(1.5) **Example.** There is one isogeny class $\mathcal{A}_{15}$ of conductor 15 which consists of 8 elliptic curves labeled A through H in the Antwerp tables. We record the partial ordering on $\mathcal{A}_{15}$ by replacing the graph of cyclic isogenies by the directed graph of étale isogenies:



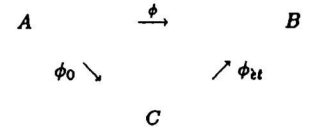
Note that while A is the only minimal element of $\mathcal{A}_{15}$, there are 4 maximal elements. In particular, $\mathcal{A}_{15}$ does not have the least upper bound property.

The proof of Theorem 1.2 is based on the following lemma which is proved in [5].

(1.6) Lemma.

(a) If $\phi : A \to B$ and $\psi : B \to C$ are $\mathbf{Q}$-isogenies then $\psi \circ \phi$ is étale if and only if both ϕ and ψ are étale.

(b) Every cyclic isogeny $\phi : A \to B$ has a unique (up to signs) factorization $\phi = \phi_{\acute{e}t} \circ \phi_0$



where both $\phi_{\acute{e}t}$ and the dual isogeny $\check{\phi}_0$ of ϕ_0 are étale. ∎

Proof of Theorem 1.2. Let $A, B \in \mathcal{A}$. Let $\phi : A \to B$ be a cyclic isogeny, and let $\phi = \phi_{\acute{e}t} \circ \phi_0$ be the factorization whose existence is guaranteed by (1.6)(b). Since $\check{\phi}_0 : C \to A$ and $\phi_{\acute{e}t} : C \to B$ are étale we see that $\mathcal{L}(C) \subseteq \mathcal{L}(A) \cap \mathcal{L}(B)$. Equality is an easy consequence of the cyclicity of ϕ. ∎

§2 The Optimal Lattice

In this section we assume that $\mathcal{A}$ is an isogeny class of *modular* elliptic curves. This means that there is a weight two newform f whose L-series $L(f, s)$ is equal to the L-series of $\mathcal{A}$. The level N of f is equal to the conductor of $\mathcal{A}$ [1]. The differential form $\omega_f = 2\pi i f(z)dz$ on the upper half plane is invariant under $\Gamma_0(N)$ and descends to a holomorphic 1-form on the complete modular curve $X_0(N)$. Similarly, if $\Gamma \subseteq \Gamma_0(N)$ is an arbitrary congruence subgroup then ω_f defines a regular 1-form on the complete modular curve X_Γ associated to Γ. By integrating ω_f over 1-cycles on X_Γ we obtain a group of periods $\mathcal{L}_\Gamma(f) \subseteq \mathbf{C}$. Since f is an eigenform for the Hecke operators with rational eigenvalues, we know that $\mathcal{L}_\Gamma(f)$ is a lattice. Define

$$\mathcal{L}(f) \stackrel{def}{=} \bigcap \mathcal{L}_\Gamma(f)$$

where the intersection is over all congruence subgroups $\Gamma \subseteq \Gamma_0(N)$.

(2.1) Theorem. *Let f be the weight two newform associated to an isogeny class of modular elliptic curves of conductor N. Then $\mathcal{L}(f) = \mathcal{L}_{\Gamma_1(N)}(f)$. In particular, $\mathcal{L}(f)$ is a lattice.*

Proof. Define the homomorphism $\Phi : \Gamma_0(N) \to \mathbf{C}$ by $\Phi(\gamma) = \int_z^{\gamma z} \omega_f$ where z is an arbitrary point in the upper half plane. Then for each congruence subgroup Γ of $\Gamma_0(N)$ we have $\Phi(\Gamma) = \mathcal{L}_\Gamma(f)$. Since f is a cusp form, $\Phi(\gamma) = 0$ for every parabolic element $\gamma \in \Gamma_0(N)$. A theorem of Fricke and Wohlfahrt [7] shows that $\Gamma_1(N)$ is generated by its parabolic elements together with any congruence subgroup. Thus $\mathcal{L}_\Gamma(f) = \mathcal{L}_{\Gamma_1(N)}(f)$ for any congruence subgroup $\Gamma \subseteq \Gamma_1(N)$. The theorem follows at once. ∎

(2.2) Definition. The lattice $\mathcal{L}(f)$ is called the *optimal lattice* of $\mathcal{A}$.

The basic conjecture which we propose to study is as follows.

(2.3) **Conjecture.** *Let A be an isogeny class of modular elliptic curves. Then the minimal and optimal lattices of A are identical:* $\mathcal{L}(A_{min}) = \mathcal{L}(f)$. ∎

§3 Evidence for the Conjecture.

We summarize the evidence for Conjecture 2.3 in the following theorem.

(3.1) **Theorem.** *Let A be a* Q*-isogeny class of modular elliptic curves.*

(a) Let ψ be a quadratic Galois character which is unramified at the primes where A has additive reduction. If Conjecture 2.3 is true for A then it is also true for the twisted isogeny class A^{ψ}.

(b) If A has complex multiplication by an imaginary quadratic field with only two roots of unity, then up to a factor of 2 Conjecture 2.3 is true for A. More precisely, either $\mathcal{L}(A_{min}) = \mathcal{L}(f)$ or $\mathcal{L}(A_{min}) = 2 \cdot \mathcal{L}(f)$.

(c) Conjecture 2.3 is true for all 281 isogeny classes listed in the Antwerp tables [6].

The proof of (c) is accomplished by direct calculation, on a Macintosh Plus personal computer, of the minimal and optimal lattices of each isogeny class in the Antwerp tables. Complete proofs of (a) and (b) can be found in [5]. It is interesting to note that the proof of (b) is based on a theorem of Rubin [3] concerning the integrality of certain special values of L-functions. Thus the proof of (b) provides another example of the interplay between Conjecture 2.3 and the arithmetic of values of L-functions.

Department of Mathematics
Boston University
Boston, MA 02215
U.S.A.

Research supported by the National Science Foundation.

REFERENCES

[1] Carayol, H.: Sur les representations ℓ-adiques attachées aux formes modulaires de Hilbert. *C.R. Acad. Sci. Paris Sér. I Math.* **296** (1983), no.15, 629-632.

[2] Cox, D.: Gauss and the arithmetic-geometric mean. *Notices of the A.M.S.* **32** (1985), 147-151.

[3] Rubin, K.: Congruences for special values of L-functions of elliptic curves with complex multiplication. *Invent. Math.* **71**, 339-364 (1983).

[4] Shimura, G.: Introduction to the arithmetic theory of automorphic forms. *Publications of the Mathematical Society of Japan* 11. Princeton: Princeton University Press 1971.

[5] Stevens, G.: Stickelberger elements and modular parametrizations of elliptic curves. To appear.

[6] Swinnerton-Dyer, et al.: Table 1; Modular functions of one variable, *Lect. Notes in Math* **476** (1975), 81-113.

[7] Wohlfahrt, K.: An extension of F. Klein's level concept. *Illinois J. Math.* **8**, 529-535 (1964).

Received April 29, 1988

An involutive automorphism of the Bunce-Deddens algebra

A. Kumjian

Presented by G.A. Elliott, F.R.S.C.

Very recently Blackadar has shown the existence of a period two automorphism of the CAR algebra for which the fixed point algebra is not AF [B2]. Motivated by his example we show that the crossed-product of the Bunce-Deddens algebra of type 2^∞ by the involutive automorphism which acts on the unit circle by complex conjugation is AF (the K-theory of this crossed-product may be found in [B1, 10.11.5c]). That this was likely to be true was suggested in personal correspondence from Blackadar. The methods used in the proof can be modified to verify the analogous result for any Bunce-Deddens algebra, but in the interests of brevity and ease of exposition we restrict ourselves to the case mentioned.

Let $\mathbf{T} = \mathbf{R}/\mathbf{Z}$ and $\mathbf{D}$ denote the dyadic rationals mod 1; we view $\mathbf{D}$ as a subgroup of $\mathbf{T}$ in the obvious way. Thus, $\mathbf{D}$ acts on $C(\mathbf{T})$ by translation and the resulting crossed-product $C(\mathbf{T}) \times_\tau \mathbf{D}$, where $\tau_d f(x) = f(x-d)$, is the well-known Bunce-Deddens algebra of type 2^∞ (see [BD],[G]). For $f \in C(\mathbf{T})$ set $\sigma f(x) = f(-x)$; clearly, $\sigma^2 = 1$ and $\sigma \tau_d \sigma = \tau_{-d}$. We show below that the resultant crossed-product, $C(\mathbf{T}) \times_\tau \mathbf{D} \times_\sigma \mathbf{Z}_2$, is AF by showing that elements of this algebra may be approximated by elements of certain finite-dimensional subalgebras in a controlled way (see [Br, 2.2]). The heart of the proof lies in the construction of these subalgebras.

We construct a finite-dimensional subalgebra, A_n, of the algebra, $C(\mathbf{T}) \times_\tau \mathbf{Z}_{2^n} \times_\sigma \mathbf{Z}_2$, generated by $C(\mathbf{T})$ and unitaries, u,v, where u is the unitary implementing translation by 2^{-n} and v is the unitary implementing σ. Fix δ with $0 < \delta < 1/2^{n+1}$ and set $\theta_k = (2k+1)/2^{n+1}$. Note that θ_k is a fixed point of the homeomorphism of $\mathbf{T}$ associated to the automorphism $\mathrm{Ad}\, u^{2k+1}v$.

For $x \in [\theta_k - \delta, \theta_k + \delta]$ set $\varphi_k(x) = (\theta_k + \delta - x)/2\delta$ and define $f_k \in C(\mathbf{T})$ by

$$f_k(x) = \begin{cases} 1 - \varphi_{k-1}(x) & \text{if } \theta_{k-1} - \delta \le x \le \theta_{k-1} + \delta \\ 1 & \text{if } \theta_{k-1} + \delta < x < \theta_k - \delta \\ \varphi_k(x) & \text{if } \theta_k - \delta \le x \le \theta_k + \delta \\ 0 & \text{elsewhere;} \end{cases}$$

and define $g_k \in C(\mathbf{T})$ by

$$g_k(x) = \begin{cases} (\varphi_k(x)(1 - \varphi_k(x)))^{1/2} & \text{if } \theta_k - \delta \le x \le \theta_k + \delta \\ 0 & \text{elsewhere.} \end{cases}$$

Finally, set

$$p_k = f_k + (-1)^k (u^{2k+1} v g_k + u^{2k-1} v g_{k-1}).$$

One verifies that p_k is a projection for $k = 0, \ldots, 2^n - 1$ (see [R, 1.1]) and that

$$\sum_{k=0}^{2^n-1} p_k = 1.$$

Moreover,

$$vp_k v = p_{-k},$$

$$u^{2j} p_k u^{-2j} = p_{k-2j}.$$

The subalgebra generated by the projections, p_k, and the unitaries, u^2 and v, is easily seen to be finite dimensional (in fact, it is isomorphic to the direct sum of four copies of $M_{2^{n-1}}(\mathbf{C})$); denote this subalgebra by A_n.

To show that $C(\mathbf{T})\times_\tau \mathbf{D}\times_\sigma \mathbf{Z}_2$ is AF, it suffices to show that any diagonal element, $f \in C(\mathbf{T})$, may be approximated by an element in A_n (for n sufficiently large). This is because arbitrary elements may be approximated by elements of the subalgebras, $C(\mathbf{T})\times_\tau \mathbf{Z}_{2^m} \times_\sigma \mathbf{Z}_2$, which in turn may be written as finite sums of terms of the form, wh, where w is a unitary (in A_n for $n > m$) and $h \in C(\mathbf{T})$. Suppose that n has been chosen so that $|f(x) - f(y)| \leq \epsilon$ when $|x - y| \leq 2^{-n}$. Set $\lambda_k = f(\frac{k}{2^n})$; the reader may wish to check that

$$\left\| f - \sum_{k=0}^{2^n-1} \lambda_k p_k \right\| \leq 2\epsilon.$$

References

[B1] B. Blackadar, K-theory for Operator Algebras, MSRI Publications v. 5, Springer-Verlag, New York, Berlin, Heidelberg, London, Paris, Tokyo, 1986

[B2] B. Blackadar, Symmetries of the CAR algebra, preprint (preliminary version)

[Br] O. Bratteli, Inductive limits of finite-dimensional C^*-algebras, Transactions Amer. Math. Soc., 171 (1972), 195-234

[BD] J. Bunce and J. Deddens, A family of simple C^*-algebras related to weighted shift operators, J. Functional Analysis, 19 (1975), 13-24

[G] P. Ghatage, C^*-algebras generated by weighted shifts, Indiana Univ. Math. J., 30 (1981), 539-545

[R] M. A. Rieffel, C^*-algebras associated with irrational rotations, Pacific J. Math., 93 (1981), 415-429

Department of Mathematics
University of Nevada
Reno, NV 89557

Received June 16, 1988

MEASURE-VALUED LIMITS FOR SOME EXCHANGEABLE SYSTEMS OF PARTICLES

J. Vaillancourt*

Presented by D.A. Dawson, F.R.S.C.

ABSTRACT

Necessary and sufficient conditions are given for the solution of a large class of martingale problems on $C([0,\infty) : (\mathcal{R}^d)^m)$ to be m-exchangeable, in terms of the drift and diffusion coefficients. Under some mild growth conditions, the sequence of empirical measures associated with a triangular array of exchangeable diffusions is tight, thereby proving the existence of "random McKean-Vlasov limits".

1. EXCHANGEABLE SYSTEMS OF PARTICLES

With $S = \mathcal{R}^d$ and m the number of particles in some finite system, let $L_m : C_c^\infty(S^m) \to C(S^m)$ be defined by

$$L_m := \frac{1}{2}(\underline{a}\nabla)^T\nabla + \underline{b}^T\nabla$$

where $\underline{b} : S^m \to S^m$ is continuous, $\underline{a}$ is continuous from S^m to the space of real $md \times md$ symmetric positive definite matrices and, for some $K > 0$,

$$|\underline{a}(x)| + |\underline{b}(x)|^2 \leq K(1 + |x|^2)$$

holds for all $x \in S^m$.

Under these conditions, the martingale problem for L_m is well-posed on $C([0,\infty) : S^m)$ (see [6] p.255) and the unique solution set $\{P_y^m : y \in S^m\}$ is called the diffusion (measure) generated by operator L_m.

* Research supported by NSERC.

The family $\{P_y^m : y \in S^m\}$ will be called (m-)exchangeable if it satisfies

$$P_{\Pi y}^m = P_y^m \circ \tilde{\Pi}^{-1}$$

for every $y \in S^m$ and every $\pi \in perm(m)$, the set of all permutations of $\{1, 2, \ldots, m\}$, with

$$\Pi y = \Pi(y_1, y_2, \ldots, y_m) := (y_{\pi 1}, y_{\pi 2}, \ldots, y_{\pi m}) \quad \text{for each} \quad y \in S^m$$

and the corresponding

$$\tilde{\Pi}(w)(t) := \Pi(w(t)) \quad \text{for each} \quad w \in C([0, \infty) : S^m).$$

1.1 **THEOREM.** Under the conditions stated above on L_m, the family $\{P_y^m : y \in S^m\}$ is exchangeable if and only if

$$1.2 \quad \begin{cases} b_i(\Pi y) & = b_{\pi i}(y) \\ a_{ij}(\Pi y) & = a_{\pi i \pi j}(y) \end{cases}$$

hold for all $i, j = 1, 2, \ldots, m$, $y \in S^m$, $\pi \in perm(m)$ and corresponding $\Pi : S^m \to S^m$.

Sufficiency is a consequence of the uniqueness of solution to the martingale problem; necessity follows from an application of the bounded convergence theorem in the martingale formulation.

REMARK: If we put $\mu_m := \frac{1}{m} \sum_{i=1}^m \delta_{y_i} \in \mathcal{P}(S)$, the space of probability measures on S (endowed with the weak topology), then any pair $(\underline{a}, \underline{b})$ satisfying (1.2) corresponds uniquely to some triple (b, σ, ρ) such that the following holds everywhere:

$$1.3 \quad \begin{cases} b_i(y) = b(y_i, \mu_m) \\ a_{ii}(y) = \sigma(y_i, \mu_m) \\ a_{ij}(y) = \rho(y_i, y_j, \mu_m) \end{cases} \quad \text{for all } i, j = 1, 2, \ldots, m, \ i \neq j.$$

2. THE EXISTENCE OF "RANDOM McKEAN-VLASOV LIMITS" FOR EXCHANGEABLE DIFFUSIONS

Let $X^m(t) = (X_i^m(t))_{i=1}^m$ denote the S^m-valued canonical process associated with the martingale problem for L_m and denote the corresponding empirical measure by $\Phi_m(X^m)(t) := \frac{1}{m}\sum_{i=1}^m \delta_{X_i^m(t)}$. There exists weak limits to the sequence Φ_m for a very large class of exchangeable diffusions, encompassing several of those in [1], [4] and [5], where the limits are deterministic evolutions in $\mathcal{P}(S)$. In many cases here, the evolutions are random.

Following [2], we denote $F_f(\mu) := \int_{S^k} f d\mu^{\times k}$ where $f \in C(S^k)$ for some $k \geq 1$ and $\mu^{\times k}$ is the k-fold product of measure $\mu \in \mathcal{P}(S)$ by itself. A computation yields that

$$P_y^m \circ \Phi_m^{-1} \in \mathcal{P}(C([0,\infty) : \mathcal{P}(S)))$$

is a solution to the martingale problem for $\mathcal{L}_m$, started at $\frac{1}{m}\sum_{i=1}^m \delta_{y_i}$, where

$$\mathcal{L}_m F_f(\mu) := F_{A_k(\mu)f}(\mu) + \frac{1}{2m} F_{B_k(\mu)f}(\mu)$$

with

$$A_k(\mu)f(y) := \sum_{\alpha=1}^k b^T(y_\alpha,\mu)\nabla_\alpha f(y) + \frac{1}{2}\sum_{\alpha=1}^k (\sigma(y_\alpha,\mu)\nabla_\alpha)^T\nabla_\alpha f(y)$$
$$+ \frac{1}{2}\sum_{\substack{\alpha,\beta=1\\ \alpha\neq\beta}}^k (\rho(y_\alpha,y_\beta,\mu)\nabla_\beta)^T\nabla_\alpha f(y),$$

$$B_k(\mu)f(y) := \sum_{\substack{\alpha,\beta=1\\ \alpha\neq\beta}}^k \left((\sigma(y_\alpha,\mu) - \rho(y_\alpha,y_\beta,\mu))\nabla_\beta\right)^T\nabla_\alpha f(y_{\alpha\beta}),$$

$$y_{\alpha\beta} = (y_1, y_2, \ldots, y_{\beta-1}, y_\alpha, y_{\beta+1}, \ldots, y_m),$$

for all $k \geq 1$ and all $f \in C_c^\infty(S^k)$.

2.1 **THEOREM.** Let $b : S \times \mathcal{P}(S) \to S$, $\sigma : S \times \mathcal{P}(S) \to S \otimes S$ and $\rho : S \times S \times \mathcal{P}(S) \to S \otimes S$ be continuous functions such that the following hold:

(i) There exists a $K > 0$ such that, for every $x, y \in S$ and $\mu \in \mathcal{P}(S)$,

$$|b(x,\mu)|^2 + |\sigma(x,\mu)|^2 \leq K(1 + |x|^2)$$

and

$$|\rho(x,y,\mu)| \leq K(1 + |x|^2 + |y|^2).$$

(ii) For each $m \geq 1$ and each $y^m \in S^m$, the matrix $a^m(y^m) \in S^m \otimes S^m$ defined by (1.3) is positive definite and symmetric.

(iii) For each $m \geq 1$, $\nu^m \in \mathcal{P}(S^m)$ is such that the coordinates are exchangeable random variables and $\sup_m \int |x_1|^4 \nu_m(dx) < \infty$.

then $\{P^m_{\nu^m} \circ \Phi_m^{-1} : m \geq 1\} \subset \mathcal{P}(C([0,\infty) : \mathcal{P}(\overline{S})))$ is tight.

The proof is an application of the results of Joffe and Métivier[3] on the weak convergence of D-semimartingales. That condition (ii) of Theorem (2.1) is not really too restrictive may be readily observed from the following result:

2.2 **COROLLARY.** Let $b : \mathcal{P}(S) \to S$ and σ, $\rho : \mathcal{P}(S) \to S \otimes S$ be bounded continuous functions such that σ and ρ satisfy the following conditions:

(i) $\sigma(\mu)$, $\rho(\mu)$ are symmetric for every $\mu \in \mathcal{P}(S)$;

(ii) $\rho(\mu)$ and $\sigma(\mu) - \rho(\mu)$ are positive definite for every $\mu \in \mathcal{P}(S)$;

(iii) Condition (iii) of Theorem (2.1) holds;

then the conclusion of Theorem (2.1) holds.

We finally obtain the existence result sought via the martingale formulation (and the fact that the conditions ensure non-explosion).

2.3 **THEOREM.** Let b, σ, ρ satisfy the conditions (i) and (ii) of Theorem (2.1); then, for any $\mu \in \mathcal{P}(S)$ with $\int |x|^4 d\mu(x) < \infty$, there is a solution to the martingale problem for L_∞ in $\mathcal{P}(C([0,\infty) : \mathcal{P}(S)))$, started at μ, with $L_\infty F_f(\mu) := F_{A_k(\mu)f}(\mu)$ for all $k \geq 1$ and $f \in C_c^\infty(S^k)$.

REMARK: The method of duality has been successfully used in [2] to prove the uniqueness of solution when b, σ and ρ are independent of μ and satisfy the conditions of Theorem (2.3). In [1], [4] and [5], where the unique limit is deterministic, the characterization is obtained by proving the uniquemess of solution to the associated nonlinear McKean-Vlasov equations.

ACKNOWLEDGEMENT

The author wishes to thank Professor D.A.Dawson for many valuable suggestions made throughout the course of this work.

REFERENCES

[1] Dawson, D.A., Critical Dynamics and Fluctuations for a Mean-Field Model of Cooperative Behavior, Journal of Statistical Physics 31,1(1983),pp.29-84.

[2] Dawson, D.A. and Kurtz, T.G., Applications of Duality to Measure-Valued Processes, in Lecture Notes in Control and Information Sciences 42(1982),pp.177-191.

[3] Joffe, A. and Métivier, M., Weak Convergence of Sequences of Semimartingales with Applications to Multitype Branching Processes, Advances in Applied Probability 18(1986),pp.20-65.

[4] Léonard, C., Une Loi des Grands Nombres pour des Systèmes de Diffusions avec Interactions et Coefficients Non Bornés, Ann.Inst.H.Poincaré 22,2(1986), pp.237-262.

[5] Oelschläger, K., A Martingale Approach to the Law of Large Numbers for Weakly Interacting Stochastic Processes, Annals of Probability 12,2(1984),pp.458-479.

[6] Stroock, D.W. and Varadhan, S.R.S., Multidimensional Diffusion Processes, Springer-Verlag(1979).

Département de Mathématique et Informatique,
Université de Sherbrooke,
Sherbrooke, Canada, J1K 2R1.

Received June 23, 1988

M.D.S. codes and arcs in projective space I

by

A.A. Bruen, J.A. Thas and A. Blokhuis

Presented by H.S.M. Coxeter, F.R.S.C.

Foreward. For reasons of space we have had to split this paper into two parts, I and II. All of the references for Parts I, II are at the end of Part I .

Section 1. Introduction, background.

Let $V = V(k,q)$ be a vector space of dimension k over the finite field $F = GF(q)$, $q = p^h$. Let S be a set of n vectors in V such that each of the $\begin{bmatrix} n \\ k \end{bmatrix}$ k-subsets of S is a basis for V. A fundamental and much studied question can now be posed.

Question. How large can n be, and what is the structure of S in the largest case?

In this form the question dates back about thirty-five years to the work of B. Segre [14], who was able to utilize projective and algebraic geometry to obtain solutions in various special cases. The question also has its roots in a statistical problem discussed by K.A. Bush in [1] and in a part of combinatorics connected with the orthogonal arrays of R.C. Bose and others [1]. Our question is also closely related to the topic of Maximum Distance Separable codes (M.D.S. codes) which were discussed in [18] by R.C. Singleton. F.J. MacWilliams and N.J.A. Sloane [12] introduce their chapter on M.D.S. codes as "one of the most fascinating in all of coding theory". There is a voluminous literature on the subject. We refer to [12] for references as well as to the work of C. Maneri and R. Silverman [13] and to the recent book of R. Hill [9].

The main results on the question have been obtained, using geometrical methods, by B. Segre and subsequently by J.A. Thas, and by L.R.A. Casse and D.G. Glynn [see 4,5,6,8,10,11,14,15,16,19,20, 21,22]. Before describing their work we first put the problem in a wider combinatorial context.

Let C be a code of length n over an alphabet F of size q, so $|F| = q$ with q some positive integer and $q \geq 2$. In other words C is a collection of (code) words where each word is an n-tuple over F. Having chosen k with $2 \leq k \leq n$ we impose the following condition on C.

Work supported in part by the National Fund for Scientific Research (Belgium), N.A.T.O. and N.S.E.R.C. (Canada).

1980 Mathematics Subject Classification: Primary 1C05, 2K51, 2U11.

Condition 1. No two words in C agree in as many as k positions.

It follows that $|C| \leq q^k$. If $|C| = q^k$ then C is called a Maximum Distance Separable code (= M.D.S. code). If C is M.D.S. we have $d(C) = n - k + 1$ where d(C) is the minimum (Hamming) distance of C. One of the main problems concerning such codes is to maximize d(C), and so n, for given k and q.

Problem 1. For given k,q what is the maximum value of n for which such M.D.S. codes exist? And what is the structure of C in the optimal case?

For example, let $k = 2$. Then C gives a set of q^2 (code) words of length n, no two of which agree in as many as 2 positions. This is equivalent to the existence of a (Bruck) net of order q and degree n [7]. It follows that $n \leq q + 1$, the case of equality corresponding to an affine plane of order q. From this, by an inductive argument, one can show the following result.

Theorem 1. We have $n \leq q + k - 1$.

The case $k = 3$ and $n = q + 2$ is equivalent to the existence of an affine plane π of order q containing an elaborate system of hyperovals. The only known example is when π is classical so that $q = 2^h$. For $k = 4$ and $n = q + 3$ one can only show that $q = 2$ or that 36 divides q [2], q being the order of some projective plane, even though (presumably) no examples with $q > 2$ exist. At the moment an exact answer to the question of the existence and structure of a finite plane of order q seems well beyond present techniques. Accordingly, it seems that one cannot do much with Problem 1 in its present generality.

We therefore formulate the problem for the case when C is linear. It goes like this. Let C be a k-dimensional subspace of $V = V(n,q)$, a vector space of dimension n over $F = GF(q)$ where $q = p^h$ and GF(q) is the finite field of order q. Choose any basis for C and represent it as a k by n matrix X over F of rank k. Since X has rank k some set of k columns of X is linearly independent. Actually, Condition 1 now has as its analogue the following condition.

Condition 2. Every set of k columns of X is linearly independent.

Note. If we regard the columns as vectors in a k-dimensional vector space we are back to the original question.

As pointed out in Theorem 1 we already have $n \leq q + k - 1$. However since we are now dealing with a more special class of codes we expect stronger results.

As noted by B. Segre one can multiply the columns of X by non-zero scalars and still preserve the independence property. He therefore regarded the columns of X as points (or, by duality, as hyperplanes) belonging to an arc in $\Sigma = PG(k - 1,q)$, the projective space of dimension k - 1 over the field GF(q). Here an s-arc of

points (or hyperplanes) in PG(r,q) is a set A of s points (or hyperplanes) with $|A| \geq r + 1$ such that no r + 1 points (or hyperplanes) of A lie in a hyperplane (or pass through a point). An arc A is *complete* if it is not properly contained in a larger arc. Otherwise, if A ∪ {P} is an arc for some point P we say that P *extends* A. In PG(2,q) it is easy to show that $|A| \leq q + 2$: moreover, (q + 2)-arcs exist for q even [10]. In PG(2,q), q odd, we have $|A| \leq q + 1$: moreover, (q + 1)-arcs exist for q odd (see [14] and 2.3 below). In PG(q - 2,q), q even, there holds $|A| \leq q + 2$ and a (q + 2)-arc can be constructed by adjoining a certain point to the point set of a normal rational curve [20,21]. In fact the known results suggest the following tantalizing and simply stated conjecture which has remained unsolved for over thirty years.

Conjecture 1. *Assume* $(r,q) \neq (2,2^h), (2^h - 2, 2^h)$. *Then* $|A| \leq q + 1$. (Note that in $PG(2,2^h)$ *and* $PG(2^h - 2, 2^h)$ *we have* $|A| \leq q + 2$.)

In this work we describe fundamental progress on the original question: the details are in [3]. In particular our results support the conjecture.

Section 2. A sketch of known results.

Let k = 3 and B an arc (of points) in $\pi = PG(2,q)$, with $|B| = \beta$. Define a *tangent* to B to be a line of π meeting B in a unique point. By elementary but ingenious arguments [15, and 10, Chapter 10], the following results have been shown by B. Segre.

2.1 Theorem. *The tβ tangents to B* (where $t = q + 2 - \beta$) *belong to an algebraic envelope Γ where Γ has class t* (or 2t) *if q is even* (or odd) *respectively*.

With suitable conditions on β Segre goes on to establish a one to one correspondence between points of π extending B and linear factors of Γ. Using some fundamental results from algebraic geometry (e.g. Bezout's theorem, the Hasse-Weil estimates for curves) the following key result transpires [10,16,22]. (Part 2 is a slight improvement by J.A. Thas [22] of the original theorem due to B. Segre [16].)

2.2 Theorem. *Assume that* $\beta > \lambda(q)$ *where*

$$\lambda(q) = \begin{cases} q - \sqrt{q} + 1 & (q \text{ even}) \\ q - \frac{\sqrt{q}}{4} + \frac{25}{16} & (q \text{ odd}) \end{cases}.$$

Then

(1) *B is embedded in a (q + 2)-arc for q even, which is unique except when* $q = \beta = 2$.

(2) *B is embedded in a unique conic if q is odd*.

A special case of Part (2) is usually referred to as Segre's theorem.

2.3 Theorem. In PG(2,q), q odd, every (q + 1)-arc is the point set of a conic.

In particular, since, for q odd, a conic can not be extended, 2.3 implies that, for q odd, $\beta \leq q + 1$.

We emphasize that 2.3 is not valid for q even. To see this, let C be any conic in PG(2,q), $q = 2^h$. Then the tangents to C are all concurrent at a nucleus point N. Choose any point P of C and form the (q + 1)-arc $D = (C - (P)) \cup (N)$. Since any five points of an arc determine a unique conic we have that D is not the point set of a conic when $q > 4$.

Next let B be a (q + 1)-arc of points in $\Sigma = PG(3,q)$, q odd. Let P_1, P_2 be two points of B. Let $f(P_1)$, $f(P_2)$ be the projection of B onto π from P_1, P_2, where the plane π does not contain either of P_1, P_2. Then each of $f(P_1)$, $f(P_2)$ is a q-arc which, for $q > 37$, by 2.2 Part (2) is embedded in a unique conic C_1, C_2 respectively. Therefore, for $q > 37$, B lies on the intersection of the quadratic cone joining P_1 to C_1 with the quadratic cone joining P_2 to C_2. It can then be shown that B is the point set of a twisted cubic curve C given in coordinates by $C = \{(1,t,t^2,t^3) \cup (0,0,0,1) \mid t \text{ in } GF(q)\}$. In fact, this result holds for every odd q [14].

Pursuing this idea in the more complicated setting of higher dimensions, again using 2.2, the following has been shown by J.A. Thas [19,22].

2.4 Theorem. In $\Sigma = PG(r,q)$, with q odd and $r \geq 2$, let B be an arc with $|B| = \beta$. Then

(1) for $q > (4r - \frac{23}{4})^2$ we have $\beta \leq q + 1$,

(2) for $q > (4r - \frac{23}{4})^2$ every (q + 1)-arc is the point set of a normal rational curve in Σ,

(3) for $\beta > q - \frac{\sqrt{q}}{4} + r - \frac{7}{16}$ the arc B is contained in one and only one normal rational curve of Σ.

Recently, D.G. Glynn [8], has constructed an example of a 10-arc in PG(4,9) which is not the point set of a normal rational curve.

As noted earlier, Theorem 2.3 is not valid for q even, making this case more difficult. By a clever use of coordinates, the following is shown in [4,5].

2.5 Theorem. Let B be an arc of points in PG(3,q), $q = 2^h$. Then, for $q \neq 2$, $|B| \leq q + 1$. If $|B| = q + 1$ then B is projectively equivalent to $C = \{(1,t,t^e,t^{e+1}) \mid t \text{ in } GF(q) \cup (\infty)\}$ with $e = 2^m$ and $(m,h) = 1$.

Surprisingly it seems that this example of a "twisted" normal rational curve in 2.5 does not extend to higher dimensions. We have (see [6]).

2.6 Theorem. Let B be an arc of points in PG(4,q), $q = 2^h$. Then $|B| \leq q + 1$ for $q > 4$. If $|B| = q + 1$ then B is the point set of a normal rational curve.

REFERENCES

[1] K.A. Bush, Orthogonal arrays of index unity, Ann. Math. Stat. 3(1952), 426-434.

[2] A.A. Bruen and R. Silverman, On the non-existence of certain M.D.S. codes and projective planes, Math. Z. 183(1983), 171-175.

[3] A.A. Bruen, J.A. Thas and A. Blokhuis, On M.D.S. codes, arcs in PG(n,q) with q even, and a solution of three fundamental problems of B. Segre, Inventiones Math., to appear.

[4] L.R.A. Casse, A solution to B. Segre's problem $I_{r,q}$, VII Osterreichischer Mathematikerkongress, Linz, 1968.

[5] L.R.A. Casse and D.G. Glynn, The solution to Beniamino Segre's problem $I_{r,q}$, $r = 3$, $q = 2^h$, Geom. Dedicata 13(1982), 157-163.

[6] L.R.A. Casse and D.G. Glynn, On the uniqueness of $(q + 1)_4$-arcs of PG(4,q), $q = 2^h$, $h \geq 3$, Discrete Math. 48(1984), 173-186.

[7] P. Dembowski, Finite Geometries, Springer-Verlag, Berlin, 1968.

[8] D.G. Glynn, The non-classical 10-arc of PG(4,9), Discrete Math. 59(1986), 43-51.

[9] R. Hill, A First Course in Coding Theory, Clarendon Press, Oxford, 1986.

[10] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, Clarendon Press, Oxford, 1979.

[11] J.W.P. Hirschfeld, Finite Projective Spaces of Three Dimensions, Clarendon Press, Oxford, 1985.

[12] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.

[13] C. Maneri and R. Silverman, A combinatorial problem with applications to geometry, J. Comb. Theory A 11(1971), 118-121.

[14] B. Segre, Curve razionali normali e k-archi negli spazi finiti, Ann. Mat. Pura Appl. 39(1955), 357-379.

[15] B. Segre, Lectures on Modern Geometry, Ed. Cremonese, Roma, 1961.

[16] B. Segre, Introduction to Galois Geometries, Mem. Accad. Naz. Lincei 8(1967), 133-236.

[17] G. Seroussi and R.M. Roth, On M.D.S. extensions of generalized Reed-Solomon codes, IEEE Trans. Infor. Theory, to appear.

[18] R.C. Singleton, Maximum distance q-nary codes, IEEE Trans. Infor. Theory 10(1964), 116-118.

[19] J.A. Thas, Normal rational curves and k-arcs in Galois spaces, Rend. Mat. (6) 1 (1968), 331-334.

[20] J.A. Thas, Connection between the Grassmannian $G_{k-1;n}$ and the set of the k-arcs of the Galois space $S_{n,q}$, Rend. Mat. (6) 2 (1969), 121-134.

[21] J.A. Thas, Normal rational curves and (q + 2)-arcs in a Galois space $S_{q-2,q}$($q = 2^h$), Rend. Accad. Naz. Lincei 47(1969), 249-252.

[22] J.A. Thas, Complete arcs and algebraic curves in PG(2,q), J. Algebra, 106(1987), 451-464.

Received June 29, 1988

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF WESTERN ONTARIO
LONDON, ONTARIO, N6A 5B7
CANADA

SEMINAR OF GEOMETRY AND COMBINATORICS
STATE UNIVERSITY OF GHENT,
KRIJGSLAAN 281, B-9000.
GHENT, BELGIUM

DEPARTMENT OF MATHEMATICS
TECHNICAL UNIVERSITY OF EINDHOVEN
EINDHOVEN, THE NETHERLANDS

Mailing Addresses

1. A. Blokhuis — Department of Mathematics, Technical University of Eindhoven, Eindhoven, The Netherlands

2. A.A. Bruen — Department of Mathematics, University of Western Ontario, London, Ontario, N6A 5B7

3. A. Kumjian — Department of Mathematics, University of Nevada, Reno, NV 89557 U.S.A.

4. G. Stevens — Department of Mathematics, Boston University, Boston, MA 02215 U.S.A.

5. J.A. Thas — Seminar of Geometry and Combinatorics, State University of Ghent, Krijgslaan 281, B-9000, Ghent, Belgium

6. J. Vaillancourt — Département de Mathématique et Informatique, Université de Sherbrooke, Sherbrooke, Quebec, J1K 2R1