CIRCULANTS (Extract)

Alun Wyn-jones

Last revised in December 2013.

Chapter 9.
Application: Diffusion in Toroidal Spaces.

9.1 **Diffusion of Matter.** Imagine a density of matter in a space, T. Let the density function at time t be $f_t(x)$. Let the quantity of matter in the neighborhood of y moved to a neighborhood of x of equal volume in a small time interval t to $t+h$ be $a_{t,h}(x, y, f_t(y))$. Then the equation for the diffusion in the small time interval t to $t+h$ is

$$f_{t+h}(x) \;=\; \int_T a_{t,h}\left(x, y, f_t(y)\right) dy$$

We shall now make various simplifying assumptions. The first three are crucial and cannot be relaxed.

9.1.1 **The diffusion is linear.**
That is, the quantity of matter in the neighborhood of y moved to a neighborhood of x of equal volume in a small time interval t to $t+h$ is proportional to the density of matter at y at time t.

$$\therefore \;\; a_{t,h}\left(x, y, f_t(y)\right) = a_{t,h}(x, y) f_t(y)$$

9.1.2 **The diffusion is homogenous in space.**
This means that the quantity of matter moved from y to x depends only on the relative positions of x and y.

$$\therefore \;\; a_{t,h}(x, y) = a_{t,h}(x - y)$$

9.1.3 **The diffusion is homogenous in time.**
That is, the diffusion law does not vary with time. Combined with spatial homogeneity of 9.1.2, this implies

$$a_{t,h}(x - y) = a_h(x - y)$$

9.1.4 **Discrete Approximation** If the space is continuous then all distributions of interest and the diffusion law can be approximated as closely as desired with a discrete space and diffusion law.

9.1.5 **The diffusion is non-negative.** That is, if the distribution is initially non-negative then it remains non-negative for all later times. This can be guaranteed only by making the diffusion function non-negative everywhere (and by homogeneity in time, for all times).

$$\therefore \;\; a_h(x - y) \geq 0, \qquad \forall h, x, y$$

9.1.6 **Conservation of Matter**
Conservation means that $\int_T f_t(x)dx$ is constant in time. This is guaranteed if

$$\int_t a_h(y)dy = 1$$

These assumptions simplify the diffusion equation to

$$f_{t+h}(x) \;=\; \int_T a_h(x - y) f_t(y) dy$$
$$\text{with} \quad \int_T a_h(y)dy = 1$$
$$\text{and } a_h(y) \geq 0, \qquad \forall y \in T$$

9.2 **Transitions Between States.**

Another physical system that often satisfies the above assumptions is a collection of transitions between the various states of a system. The distribution now represents a probability density and the $a(x, y)$ represents the transition probability from the state y to the state x. This system automatically satisfies the assumptions 9.1.5 and 9.1.6, and it will satisfy 9.1.1 in a classical system containing only a single particle. Many such systems are inherently discrete and therefore also satisfy assumption 9.1.4.

9.3 **Circulant Matrix Model** An important question is whether any initial distribution eventually becomes equidistributed throughout the space. The special case when the space, T, is toroidal can be treated with circulant matrices. We shall first concentrate on the one-dimensional torus, the circle.

If the space is continuous then we take sufficient points in the space to approximate the continuous distributions and diffusion law. Then, with N points in the space, at the $(n+1)^{\text{th}}$ time step,

$$f_{n+1}(i) \;=\; \sum_{j\in\mathbb{Z}_N} a(i-j)f_n(j) \quad \text{where} \sum_{j\in\mathbb{Z}_N} a(j) = 1$$

Hence, the diffusion is given by multiplying the vector of densities by the circulant matrix $A_{i,j} = a(i-j)$. Normally, we shall represent the diffusion matrix by $a \in \mathbf{circ}_N(\mathbb{R})$ rather than the matrix itself. We shall need to use the matrix only when discussing its effect on the distribution vector, $f \in \mathbb{R}^N$.

Eventual equidistribution now depends on whether

$$A^r f \to f_{eq} \;:=\; (\bar{f}, \bar{f}, \ldots, \bar{f}) \quad \text{as } r \to \infty$$

$$\text{where } \bar{f} \;=\; \text{average value of } f_i \;=\; \frac{1}{N}\left(\sum_i f_i\right)$$

Since the term "eventual equidistribution" refers to a limit on vectors, we need to specify a metric on vectors. We shall adopt the dot inner-product norm since this makes the standard basis orthonormal. The dot inner-product will be written as $x.y$. Recall that the standard basis for the eigenspace is $\{e_i, \vdash\ i \in \mathbb{Z}_N\}$ which are the orthonormal eigenvectors of the circulant matrices.

In this section, the circulant matrix A is assumed conservative; that it satisfies §9.1.6. Hence, $\lambda_0(A) = 1$.

9.3.1 **Proposition** $A^r f$ approaches equidistribution iff $|\lambda_i(A)| < 1$ whenever $i > 0$ and $e_i.f \neq 0$.

Proof. First suppose that $|\lambda_i(A)| < 1$ whenever $i > 0$ and $e_i.f \neq 0$.

Let $f = \sum_{i\in\mathbb{Z}_N} f'_i e_i$, then $A^r f \;=\; \sum_{i\in\mathbb{Z}_N} \lambda_i^r f'_i e_i$. The stated conditions imply that

$$A^r f \;\to\; \lambda_0^r f'_0 e_0 \;=\; f'_0 e_0 \;\text{ as }\; r \to \infty \tag{1}$$

The eigenvectors $e_0, e_1, \ldots, e_{N-1}$ are an orthonormal set, and $e_0 = \sqrt{N^{-1}}(1, 1, \ldots, 1)$. Therefore, $f'_0 \;=\; f.e_0 \;=\; \frac{1}{\sqrt{N}} \sum_{i\in\mathbb{Z}_N} f_i$.

Hence, $A^r f$ approaches the vector $f_{eq} \;:=\; f'_0 e_0 \;=\; \frac{1}{N}\left(\sum_i f_i\right)(1, 1, \ldots, 1)$. This vector clearly represents an equidistribution. Note that the equidistributed vector, $f_{eq} = \lambda_0(f)\bar{\delta}^N$ where $\bar{\delta}^N$ is the idempotent of §3.5.

Conversely, suppose that $A^r f$ approaches equidistribution. This means that $A^r f \to f_{eq}$ as $r \to \infty$. But, f_{eq} is in the subspace spanned by e_0. Therefore, all components of f orthogonal to this subspace must tend to zero as $r \to \infty$. By equation (1), this is possible only if $\lambda_i^r f'_i \to 0$ which means either $f'_i = 0$ or $|\lambda_i| < 1$. □

The distribution will also approach equidistribution, regardless of the initial distribution, if A^r approaches the matrix O where $O_{i,j} = 1/N,\ \forall i,j$ as $r \to \infty$. If $A = \mathrm{CIRC}_N(a)$, then this is equivalent to $a^r \to \bar{\delta}^N$. We shall now investigate this possibility. We shall say that a is eventually an equidistribution circulant (or operator) if $a^r \to \bar{\delta}^N$ as $r \to \infty$. We shall make one simplifying assumption, namely the condition of 9.1.5 that the diffusion is non-negative: $a_i \geq 0$ for all i.

9.3.2 **Definition** To avoid continually repeating the conditions on a, we shall say that $a \in \mathbf{circ}_N(\mathbb{R})$ is **standard** iff $\sum_j a_j = 1$ and $a_i \geq 0,\ \forall i$. If $a_i > 0,\ \forall i$ then we shall say that a is **standard positive**.

9.3.3 **Definition** For all $c \in \mathbb{R}^N$, let $M(c) := \max_i |c_i|$ and let $m(c) := \min_i |c_i|$.
Of course, as sets, $\mathbf{circ}_N(\mathbb{R}) = \mathbb{R}^N$. So, this definition applies to $c \in \mathbf{circ}_N(\mathbb{R})$.

9.3.4 **Lemma** Let $a, b \in \mathbf{circ}_N(\mathbb{R})$ with a standard. Then, $M(ab) \leq M(b)$ and $m(ab) \geq m(b)$.

Proof. $|(ab)_i| = \left|\sum_{j\in\mathbb{Z}_N} a_j b_{i-j}\right| \leq \sum_{j\in\mathbb{Z}_N} a_j M(b) = M(b)$, and similarly, $|(ab)_i| \geq m(b)$. □

If we regard $M(a) - m(a)$ as a measure of deviation of a from $\bar{\delta}$ then, by setting $b = a^r$ in the lemma, we see that a^r can never deviate further from $\bar{\delta}$ as r increases. The following proposition gives sufficient conditions to ensure that $a^r \to \bar{\delta}$. First, we need to determine when $M(ab) - m(ab)$ is strictly less that $M(b) - m(b)$.

9.3.5 **Lemma** Let $a, b \in \mathbf{circ}_N(\mathbb{R})$. If a is standard positive then

$$M(ab) - m(ab) \ \leq\ (M(b) - m(b))\,(1 - 2m(a))$$

Proof. It is easy to see that $(a^r)_i > 0,\ \forall i \ \Rightarrow\ (a^{r+1})_i > 0$.
Let $c \in \mathbb{R}^N$, let $M(c) = c_g$ and let $m(c) = c_s$ for $g, s \in \mathbb{Z}_N$. Consider the inner-product $a.c$.

$$a.c \ =\ \sum_i a_i(c_i - c_g) + c_g \sum_i a_i \ =\ c_g - \sum_i a_i(c_g - c_i)$$

$$\text{Similarly, } a.c \ =\ c_s + \sum_i a_i(c_i - c_s)$$

Let $G = \{i \in \mathbb{Z}_N \vdash c_i = c_g\}$, and $S = \{i \in \mathbb{Z}_N \vdash c_i = c_s\}$. The components of c achieve their maximum absolute value on G and their minimum absolute value on S.

$$\begin{aligned} a.c \ &=\ c_g - \sum_{i\in\mathbb{Z}_N - G} a_i(c_g - c_i) \\ &=\ c_s + \sum_{i\in\mathbb{Z}_N - S} a_i(c_i - c_s) \end{aligned}$$

If $G \cap S \neq \emptyset$ then $G = S = \mathbb{Z}_N$ and there is nothing to prove. So assume that $G \cap S = \emptyset$. By well-ordering, $G, S \neq \emptyset$. In particular, $s \in \mathbb{Z}_N - G$ and $g \in \mathbb{Z}_N - S$. Therefore,

$$\begin{aligned} a.c \ &\leq\ c_g - m(a)(c_g - c_s) \\ a.c \ &\geq\ c_s + m(a)(c_g - c_s) \end{aligned} \tag{2}$$

Now let $b \in \mathbf{circ}_N(\mathbb{R})$ and set $c_j = b_{i-j}$ for some i. Then, $a.c = (ab)_i$. The inequalities (2) together imply that

$$M(ab) - m(ab) \ \leq\ (M(b) - m(b))\,(1 - 2m(a)) \quad \square$$

9.3.6 **Proposition** Let $a \in \mathbf{circ}_N(\mathbb{R})$. $\exists n > 0$ s.t. a^n is standard positive iff a^{n+i} is standard positive for all $i \geq 0$ iff $\lim_{r\to\infty} a^r = \bar{\delta}^N$.

Proof. That a^n standard positive implies that a^{n+i} is standard positive for all $i \geq 0$ follows easily from Lemma 9.3.4. Its converse is trivial.

So we can complete the proof by demonstrating the equivalence a^n standard positive iff $\lim_{r\to\infty} a^r = \bar{\delta}^N$.

Suppose a^n is standard positive. In the Lemma 9.3.5, setting $a \to a^n$ and $b \to a^r$, we see that $M(a^n a^r) - m(a^n a^r)$ decreases at least geometrically toward zero. Hence, the maximum and minimum components of a^{n+r} converge to a common limit. Since $\lambda_0(a) = 1$, we must have $\lim_{r\to\infty} a = \bar{\delta}^N$.

Conversely, if $\lim_{r\to\infty} a = \bar{\delta}^N$ then by convergence, a must be standard positive for all $r > n$ for some n. □

Proposition 9.3.6 reduces the question of whether a^r approaches the equidistribution operator to the question of whether a^r eventually becomes a standard positive circulant.

A little physical insight will guide us as to how to proceed. Consider the physical meaning of a diffusion law such as

$$a \;=\; a_{-1}\mathrm{u}^{N-1} + a_0 + a_1\mathrm{u}$$

A density of 1 initially at the point x will in the next instant be distributed among the three points $x-1,\ x$, and $x+1$. At the third instant, it will be distributed at $x-2,\ x-1,\ x,\ x+1,$ and $x+2$. It is clearly spreading out. Intuitively, it seems that if the diffusion law is local and approximately continuous, that a delta-function distribution will eventually become uniformly distributed. Now suppose that the diffusion contains some other terms as well as local diffusion terms. In other words,

$$a \;=\; a_{-1}u^{N-1} + a_0 + a_1u + \text{ other terms}$$

The points in the space which receive matter due to the initial terms in the diffusion will still to do so because of linearity and non-negativity of the diffusion. That is, additional non-negative terms can only increase the number of points which have non-zero densities at a later time instant.

9.3.7 **Lemma** Let $a = a_0 + a_s\mathrm{u}^s \in \mathbf{circ}_N(\mathbb{R})$ be standard with $a_0, a_s > 0$. Then
$\exists R > 0$ s.t. a^r is standard positive for all $r > R$ iff $\gcd(s, N) = 1$.

Proof. Let $\nu = \nu_{\bar{s}}$ where $\bar{s}s \equiv 1 \pmod N$ be the position multiplier homomorphism of §3.12. Then $\nu(a) = a_0 + a_s\mathrm{u}$.

$$\therefore\ \nu(a)^r \;=\; \sum_{i=0}^{r} \binom{r}{i} a_0^{r-i} a_s^{is} \mathrm{u}^i$$

Therefore, when $r \geq N$, all components of $\nu(a)^r$ will be non-zero. Applying ν^{-1} will only derange the components, therefore, all the components of a^r must also be non-zero.

Contrariwise, if $\gcd(s, N) = d > 1$ then a^r can only contain powers of u divisible by d. □

From this lemma and the discussion that preceded it, we deduce:

9.3.8 **Proposition** Let $a \in \mathbf{circ}_N(\mathbb{R})$ be standard. If a contains at least two non-zero components, a_i and a_j, say, such that $\gcd(i - j, N) = 1$ then a^N is standard positive and $\lim_{r\to\infty} a^r = \bar{\delta}^N$. □

9.3.9 **Corollary** Let $a \in \mathbf{circ}_N(\mathbb{R})$ be standard. If a contains at least two non-zero components, a_i and a_j, say, such that $\gcd(i - j, N) = 1$ then $|\lambda_i| < 1, \quad \forall i > 0$.

Proof. Use the above proposition to deduce that $A^r f$ approaches equidistribution for any f, and then use Proposition 9.3.1 with a generic vector f to deduce $\lambda_i < 1$ for $i > 0$. □

The proposition shows that if the circulant a has any two non-zero terms whose subscript difference is coprime to N, then a is eventually an equidistribution operator. What happens if all non-zero terms are separated at even intervals? For instance, suppose a_i is non-zero only for $i \equiv f \pmod{m}$ for some $f \in \mathbb{Z}_m$ and some $m \,|\, N$. Let $N = mn$, then we suppose that

$$a \;=\; \sum_{i=0}^{n-1} x_i \mathrm{u}_{mn}^{f+im} \qquad \text{for some } x_0, x_1, \ldots, x_{n-1} \geq 0$$

Intuitively, one would expect that the circulants a^r would tend to a circulant whose non-zero components were also evenly spaced, and that the non-zero values would be equidistributed among these components. This is so and will be proved in the next section.

The question remains of what happens to a^r when the non-zero components of a are not evenly spaced and yet no two subscripts of non-zero terms are separated by an interval coprime to N. As an example of such a circulant, take $a = 1 + \mathrm{u}^3 + \mathrm{u}^7$ with $N = 84$. A crude solution to this problem is to always to take a prime number of points in the space. This guarantees that a^r becomes an equidistribution operator if and only if a has two or more non-zero components. But this solution is often unavailable. The space might be inherently discrete and so the number of points would not be discretionary, or, as will be seen in section 9.5, approximations to higher dimensional torï demand a compound number of points in the space. These considerations call for a general answer to the question of the eventual form of a^r as $r \to \infty$.

9.4 **Boolean Circulants.** For $a \in \mathbf{circ}_N(\mathbb{R})$ standard, the question of whether a^r tends to $\bar{\delta}^N$ has been reduced to the question of whether a^r ultimately contains all positive components. The actual values of the components are irrevelant, only whether they are zero or not. So it is natural to define a Boolean function H on the non-negative reals by $H(x) = 0$ if $x = 0$ and $H(x) = 1$ otherwise; then extend H to a map on circulant vectors by $H(a) = (H(a_0), H(a_1), \ldots, H(a_{N-1}))$. Similarly, we can define H on real circulant matrices by $H(\mathrm{CIRC}_N(a)) := \mathrm{CIRC}_N(H(a))$. The circulant map H maps $\mathbf{circ}_N(\mathbb{R})$ to $\mathbf{circ}_N(\{0,1\})$. The base "ring" in the range of this map is the set $\{0,1\}$ and is not a ring. It is instead the set of logical truth values with the Boolean operations of disjunction '$\wedge$' and conjunction '$\vee$'. $H(a_i) = 1$ means that "$a_i > 0$ is true". $H(a_i) = 0$ means that "$a_i > 0$ is false" (and hence $a_i = 0$ because a is assumed standard throughout).

The matrices $H(\mathrm{CIRC}_N(\mathbb{R}))$ are examples of **Boolean circulant matrices**, and $H(\mathbf{circ}_N(\mathbb{R}))$ are **Boolean circulant vectors**. In here, we shall need only a few of the simpler properties of Boolean circulants. The interested reader may consult the article by Brink & Pretorius [BaP] for more details.

The operations of Boolean circulants are the same as those of circulants over rings except that the scalar operations are different. The scalar addition is conjunction whose rules are: $0 \vee x = x \vee 0 = x$, $x \vee x = x$ (which is why it is not ring addition). The scalar multiplication is disjunction whose rules are: $0 \wedge x = x \wedge 0 = 0$, $x \wedge x = x$. These rules give the rules for Boolean circulant operations. There is another way to picture the result of circulant operations on Boolean circulants. Regard the Boolean circulants as real circulants, perform the circulant operations as if on real circulants with real arithmetic, and apply the H function. In other words,

$$H(a) \wedge H(b) \;=\; H(ab), \quad \text{and} \quad H(a) \vee H(b) \;=\; H(a+b), \qquad \forall \text{ standard } a, b \in \mathbf{circ}_N(\mathbb{R})$$

Thus, we can investigate the question of whether all the circulant components in a^n become positive for some n by looking at the evolution of the Boolean circulant $H(a^n) = H(a)^{\wedge n}$ (disjunction n times).

Temporarily regard the Boolean circulants as just abstract vectors of zeroes and ones with Boolean operations. We can regard these vectors as representing subsets of $\mathbb{Z}_N$ as follows. The subset corresponding to the Boolean vector v is defined to be the subscripts of all the non-zero components of v. Formally, the correspondence is given by: $\varsigma : v \mapsto \{i \in \mathbb{Z}_N \;\vdash\; v_i = 1\}$. This is clearly a two-way correspondence: Given $A \subset \mathbb{Z}_N$, we can construct $v = \varsigma^{-1}(A)$ by setting $v_i = 1$ for all $i \in A$ and all other components to zero. Hence, ς is a bijection,

$$\varsigma : \mathbf{circ}_N(\{0,1\}) \to 2^{\mathbb{Z}_N}$$

What operation on the power set $2^{\mathbb{Z}_N}$ corresponds to the disjunction of circulants in $\mathbf{circ}_N(\{0,1\})$?

To answer this question, let $a, b \in \mathbf{circ}_N(\{0,1\})$. Then, as for ordinary circulants, a and b can be represented in the standard circulant basis thus,

$$\begin{aligned} a &= a_0 + a_1\mathrm{u} + a_2\mathrm{u}^2 + \cdots + a_{N-1}\mathrm{u}^{N-1} \\ b &= b_0 + b_1\mathrm{u} + b_2\mathrm{u}^2 + \cdots + b_{N-1}\mathrm{u}^{N-1} \end{aligned}$$

where each a_i, b_i is 0 or 1.

Suppose $a_i = b_j = 1$ for some i, j. Then, the term $1\mathrm{u}^i$ appears in the expansion for a, and the term $1\mathrm{u}^j$ appears in the expansion for b. Therefore, the term $1\mathrm{u}^{i+j}$ must appear in the expansion for the product $a \wedge b$. Since Boolean addition can never turn a non-zero value to a zero, it follows that the $(i+j)^{\text{th}}$ component of $a \wedge b$ must be 1. Hence, if $i \in \varsigma(a)$ and $j \in \varsigma(b)$ then $i + j \in \varsigma(a \wedge b)$. It is easy to see that the converse also holds. If $k \in \varsigma(a \wedge b)$, then there must be some $i, j \in \mathbb{Z}_N$ with $i + j = k$ and $a_i = b_i = 1$.

Therefore, $\varsigma(a \wedge b) = \varsigma(a) + \varsigma(b)$ where the addition is the addition of subsets in the additive group of $\mathbb{Z}_N$. That is, if G is an abelian group with addition, and $X, Y \subset G$, then $X + Y$ is defined to be the subset $\{x + y \vdash x \in X,\ y \in Y\}$ of G.

To avoid needlessly repeating definitions, given any subset $X \subset \mathbb{Z}_N$, define the sequence $X_1, X_2, \ldots$ by $X_1 = X$, $X_2 = X + X$, and in general, $X_{i+1} = X + X_i$. Then $X_{i+j} = X_i + X_j,\ \forall i, j$.

9.4.1 **Lemma** Let $a \in \mathbf{circ}_N(\mathbb{R})$ be standard, let $A = \varsigma H(a)$ be its corresponding subset of $\mathbb{Z}_N$, and let $d = \gcd(A \cup \{N\})$. If $0 \in A$, then there exists n such that $A_r = d\,\mathbb{Z}_N$ for all $r \geq n$.

Proof. Let $A = \{0, c_1, c_2, \ldots, c_t\}$. The set $\{N, c_1, c_2, \ldots, c_t\}$ has highest common divisor of d. Therefore, given any integer x, there exist integers $n_0, n_1, \ldots, n_t$ such that

$$n_0 N + n_1 c_1 + n_2 c_2 + \cdots + n_t c_t \ = \ dx$$

Therefore, given any $x \in \mathbb{Z}_N$, there exist $n_1, n_2, \ldots, n_t \in \mathbb{Z}_N$ such that

$$n_1 c_1 + n_2 c_2 + \cdots + n_t c_t \ \equiv \ dx \pmod{N} \tag{3}$$

Let $r = n_1 + n_2 + \cdots + n_t$ and consider the set $A_r = A + A + \cdots + A$. From the first n_1 summands, take the residue c_1, from the next n_2 summands, take the residue c_2, and so on. Clearly, we will get the sum in congruence (3). Since $0 \in A$, the residue $dx \bmod N$ will occur in every A_{r+i} for $i \geq 0$. This shows that ultimately, every residue of the form dx is in A_r. □

The lemma can be paraphrased as follows. Let $A = \varsigma H(a)$. Suppose $0 \in A$. Let $D \triangleleft \mathbb{Z}_N$ be minimal such that $A \subset D$, then $A_r = D$ for all $r > n$ for some n.

When $d = 1$, that is, when $D = \mathbb{Z}_N$, this shows that $a^r \to \bar{\delta}^N$ as $r \to \infty$ by Proposition 9.3.6. The case when $d > 1$ is dealt with in the next lemma.

9.4.2 **Lemma** Let $a \in \mathbf{circ}_N(\mathbb{R})$ be standard with corresponding subset $A \subset \mathbb{Z}_N$. Let $\gcd(A \cup \{N\}) = d$. If $0 \in A$ then $\lim_{r\to\infty} a^r \ = \ \bar{\delta}^{N/d}$.

Proof. Since $d \,|\, N$ we can write $N = dm$. Since $A \subset d\,\mathbb{Z}_N$ there exist $b_0, b_1, \ldots, b_{m-1} \geq 0$ such that

$$\begin{aligned} a &= \sum_{i=0}^{m} b_i \mathrm{u}_{dm}^{id} \\ \therefore\ a &= \tilde{\Gamma}_m^{dm} \left(\sum_{i=0}^{m-1} b_i \mathrm{u}_m^i \right) \end{aligned}$$

$\tilde{\Gamma}_m^{dm}$ is the circulant injection homomorphism of §3.5.2. By Proposition 3.5.4 the circulant $b \in \mathbf{circ}_m(\mathbb{R})$ is standard.

Let n be the number such that $A_n = d\,\mathbb{Z}_N$.

$$a^n \;=\; \tilde{\Gamma}_m^{dm}(b^n)$$

By the Lemma 9.4.1, every $d^{\,\text{th}}$ component of a^n is positive. Therefore, b^n is standard positive. Therefore, $b^s \to \bar{\delta}^{n|n}$ as $s \to \infty$ by Proposition 9.3.6. The formula of Proposition 3.5.4 clearly shows that $\tilde{\Gamma}_m^{dm}$ is continuous. Therefore,

$$a^s \to \tilde{\Gamma}_m^{dm}\left(\bar{\delta}^{m|m}\right) \text{ as } s \to \infty$$

$$\text{Now, } \bar{\delta}^{m|m} \;=\; \frac{1}{m}\sum_{i=0}^{m-1} \mathrm{u}_m^i$$

$$\therefore\;\; \tilde{\Gamma}_m^{dm}\left(\bar{\delta}^{m|m}\right) \;=\; \frac{1}{m}\sum_{i=0}^{m-1} \mathrm{u}_{dm}^{id} \;=\; \bar{\delta}^{m|dm}$$

$$\therefore\;\; a^s \to \bar{\delta}^{m|N} \text{ as } s \to \infty \;\square$$

The final result is all but stated.

9.4.3 **Theorem** Let a be standard. Let $D \lhd \mathbb{Z}_N$ be minimal such that $\varsigma H(a)$ is in some coset $D + f$ where $f \in \mathbb{Z}_d$. Then, $a^r - \mathrm{u}^{fr}\bar{\delta}^{N/d} \to 0$ as $r \to \infty$.

Proof. We are given that $\varsigma H(a)$ is in the f coset of D. Therefore, $\varsigma H(\mathrm{u}^{-f}a)$ is in the subgroup D, and so the circulant $\mathrm{u}^{-f}a$ is in the form of the previous lemma. Hence, $(\mathrm{u}^{-f}a)^r - \bar{\delta}^{N/d} \to 0$ as $r \to \infty$. The theorem statement now follows because we can multiply throughout by u^{fr} without affecting the convergence since $|\mathrm{u}| = 1$. $\square$

To summarize, if a physical system can be accurately represented by the circulant matrix model, then the distribution must eventually become equidistributed at evenly spaced points throughout the space possibly with a constant rotational motion. It is interesting to note that if the distribution is eventually equidistributed throughout the space then any rotational motion is undetectable within the circulant model. This is because the model treats only the evolution of densities and not the motion of the constituents of the densities.

9.5 Higher-dimensional Torï.

Circulant matrices can be applied to higher dimensional torï; we shall illustrate with the two-dimensional torus. In this case, the non-homogenous diffusion law is

$$f_{t+h}(x_1, y_1) \;=\; \int_{T^2} a_h(x_1, y_1, x_2, y_2) f_t(x_2, y_2) d(x_2, y_2)$$

Let this space be approximated with $M \times N$ points, then the diffusion law is approximated by the function $a_h\left((x_1, y_1), (x_2, y_2)\right)$ and the integral becomes a matrix product Af where the matrix A is labelled by pairs of points $(x_1, y_1), (x_2, y_2) \in T^2$. If the space is homogenous then the matrix A must satisfy the condition: For all pairs $(x_1, y_1), (x_2, y_2) \in T^2$, the entry at $(x_1, y_1), (x_2, y_2)$ must equal the entry at $(0, y_1 - x_1), (0, y_2 - x_2)$. That is, A must be a tensor circulant matrix. Therefore, by Theorem 6.2.1, we must take M, N coprime and then $A \in \mathrm{CIRC}_M(\mathbb{R}) \otimes \mathrm{CIRC}_N(\mathbb{R})$.

By Theorem 6.3.1, $\mathrm{CIRC}_M \otimes \mathrm{CIRC}_N \approx \mathrm{CIRC}_{MN}$, so all the development of sections 9.3 and 9.4 apply.

9.6 **Relaxation of the Assumptions**

The assumptions 9.1.1, 9.1.2, and 9.1.4 cannot be relaxed in any meaningful way.

Assumption 9.1.3 can be abandoned completely by replacing the time sequence $a, a^2, \ldots, a^r, \ldots$ with a sequence

$$a^{(0)}, \quad a^{(0)}a^{(1)}, \quad \ldots, \quad a^{(0)}a^{(1)}\cdots a^{(r)}, \quad \ldots$$

That is, the r^{th} time step is modelled by multiplication by the r^{th} circulant matrix $A^{(r)}$. Obviously, the development of this theory will be a lot more difficult. Most probably, a gradual, perturbative change in $A^{(r)}$ as r increases would be a necessary simplification.

Assumption 9.1.5 that a is non-negative can be eliminated, but most of sections 9.3 and 9.4 become of only indirect use. This theory would probably proceed by considering conditions on a which cause a^r to become non-negative for some r.

Assumption 9.1.6 is probably the least essential provided all others are satisfied. Essentially, the theory proceeds the same but factors are introduced at the beginning to normalize $\lambda_0(a)$. These then are removed when the desired conclusion is derived. In this case, the distribution can become everywhere zero, or everywhere infinite.