Pure and Applied Mathematics Journal
2015; 4(2-1): 7-13
Published online December 24, 2014 (http://www.sciencepublishinggroup.com/j/pamj)
doi: 10.11648/j.pamj.s.2015040201.12
ISSN: 2326-9790 (Print); ISSN: 2326-9812 (Online)

Descartes' dream: Cartesian products

Keiichi Takahashi, Takayasu Kaida

Department Information and Computer Sciences, Faculty of Humanity-Oriented Science and Engineering, Kinki University, Iizuka, Fukuoka, Japan

Email address:
ktakahas@fuk.kindai.ac.jp (K. Takahashi), kaida@fuk.kindai.ac.jp (T. Kaida)

To cite this article:
Keiichi Takahashi, Takayasu Kaida. Descartes' Dream: Cartesian Products. *Pure and Applied Mathematics Journal.* Special Issue: Abridging over Troubled Water---Scientific Foundation of Engineering Subjects. Vol. 4, No. 2-1, 2015, pp. 7-13. doi: 10.11648/j.pamj.s.2015040201.12

Abstract: In the last century, especially in the last half of the century, there was the paradigm of sectionalism prevailing and sciences and engineering were divided into very small parts which are mutually independent. It was like in Babel where there was no common language to communicate. The purpose of this paper is to present one of the possible glues—the notion of Cartesian product—to stick some remotely separated parts of science and engineering together. This concept appears in various places and it will turn out that it can unify the scattered notions quite well. Our two main objectives are the interpretation of cyclic codes as polynomials and nested PSO. We make clear the meaning of polynomials through Cartesian product or rather as terminating formal power series. The latter, formal power series, is not touched in engineering disciplines but is quite useful in unifying and interpreting various notions. In particular, it will make clear the meaning of addition of polynomials. This reminds us of topologization of adéles. PSO (Particle Swarm Optimization), a developed form of genetic algorithm, has come to our attention through the papers [4], [23] and [24]. In [4], the PSO is used to find optimal choice of parameters in the FOPID. In other two papers, PSO algorithm is used in cell balancing in the Lithium-ion battery pack for EV's. Motivated by the passage on [3] that the stability is preserved by the Cartesian product of many copies of the attractor, we may conceive of the nested PSO.

Keywords: Cartesian Product, Formal Power Series, Cyclic Codes, PSO Algorithm, Nested PSO

1. Introduction

The book [5] begins with the passage

"In November 1619, René Descartes, a twenty-three-year-old Frenchman, dreamed of a world unified by mathematics, a world in which all intellectual matters could be dealt with rationality by logical computation. 18 years since then he wrote the most famous book 'Discourse'."

In [9, p.25] the author refers to the "great Cartesian Theater," meaning apparently the notion of reason as described by " Cogito ergo sum."

In this paper we are mainly concerned with his mathematically most important invention of coordinates, Cartesian product. This is so fundamental that in engineering disciplines there is misunderstanding that it is so trivial. However, we note that the mathematically trivial fact to the effect that the matrices, which are again thought of very common and trivial, are just coordinates and are regarded as embedded in the Cartesian product is not well conceived by engineers. This can be perceived when one introduces the distance (norm) of two matrices. The range of applicability of Cartesian products is so wide and diverse that we will glimpse just part of it by concrete examples.

In [3,p.44], in relation to homeostasis, a chemo-dynamical stability of a cell in a variable environment, a description is made of the equilibrium after replication. The cell is brought out of a stable regime, to become, dynamically speaking, an *attractor*, and the stability after replication is regained in a different framework: the dynamical features of the system reappear in the *multiplicity* of nearly identical cells represented by the *Cartesian product* of many copies of the attractor, and ensures the information by perpetuation.

Another instance is, surprisingly from the EV control by PSO—Particle Swarm Optimization. For details, cf. §6. A swarm is the battery stack consisting of $N = 180 \sim 216$ particles and each particle is a cell and a particle searches in the search space $\mathbb{R}^D$ with $D = 36$ for its best position $3.6V$. As mentioned in [2], there is needed the balancing of blocks to obtain the optimal output power. For this we introduce the notion of *regiment*, which is a nested PSO. This new concept is taken from the above-mentioned Carbone-Gromov description as well as the ideas of Schoenheimer on life to the effect that it is a dynamic state of body constituents [20], where a simile is given of a military regime and an adult body.

2. Cartesian Product

As is often the case, whenever one needs to construct a real entity which corresponds to an abstract system, one appeals to the Cartesian product (direct product), or the coordinates (sequences).

Definition 1. Let $\mathit{\Lambda}$ be an arbitrary index set and let X_λ $(\lambda \in \mathit{\Lambda})$ be a family of sets indexed by $\mathit{\Lambda}$. Let a be a function from $\mathit{\Lambda}$to X_λ $(\lambda \in \mathit{\Lambda})$. Then we denote the function as

$$a = (a_\lambda) = (a_\lambda)_{\lambda \in \Lambda} \tag{2.1}$$

and we often refer to this as coordinates or a sequence in case when $\mathit{\Lambda}$ is a countable set. We denote all such functions a by

$$\prod X_\lambda = \prod\nolimits_{\lambda \in \Lambda} X_\lambda = \{(a_\lambda)_{\lambda \in \Lambda}\} \tag{2.2}$$

and refer to it as the Cartesian product (or direct product) of X_λ $(\lambda \in \mathit{\Lambda})$.

Two functions with the same domain and region coincide if and only if each of their values coincide, which means that two sequences (a_λ) and (b_λ) coincide if and only if $a_\lambda = b_\lambda$ for each $\lambda \in \mathit{\Lambda}$. In the case where X_λ $(\lambda \in \mathit{\Lambda})$ are some algebraic systems with identity e_λ, then we denote the subset of $\prod X_\lambda$ consisting of those all but finite number of whose entries are the identities by $\prod X_\lambda$ and refer to it as the direct sum.

Example 1. If in (2.2), all the X_λ's are Abelian groups with unity (very often denoted 0_λ), then the Cartesian product (2.2) becomes an Abelian group with respect to componentwise addition:

$$(a_\lambda) + (b_\lambda) = (a_\lambda + b_\lambda) \text{ for each } \lambda \in \Lambda \tag{2.3}$$

with the identity (0_λ).

Example 2. If in (2.2), all the X_λ's are rings, then the Cartesian product (2.2) becomes a ring with respect to componentwise addition and multiplication:

$$\begin{gathered}(a_\lambda) + (b_\lambda) = (a_\lambda + b_\lambda),\\ (a_\lambda)(b_\lambda) = (a_\lambda b_\lambda), \text{ for each } \lambda \in \Lambda.\end{gathered} \tag{2.4}$$

In the following examples we shall give four different constructions of the complex number field. The first two uses the Cartesian product while the fourth one is of algebraic nature. The third construction depends on the quotient field of the polynomial ring and one could say that this is also related to the Cartesian product through identification of polynomials and coordinates.

Example 3. Consider the 2-dimensional space

$$\mathbb{R}^2 = \{z = (x, y) | x, y \in \mathbb{R}\}$$

and introduce the componentwise addition (translation) and the new multiplication $*$ for $z_k = (x_k, y_k),\ k = 1,2$ by

$$z_1 * z_2 = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1). \tag{2.5}$$

Then $(\mathbb{R}^2, +,*)$ forms a field, which we refer to as the field of complex numbers and denote $\mathbb{C}$.

To prove this we note that $z = (x, y) = o = (0,0)$ if and only if $(x, y) = (0,0)$, i.e. if and only if $z = o$, i.e. if and only if $|z| = \sqrt{x^2 + y^2} = 0$. Hence for each $z \neq o$, there exists the inverse element $z^{-1} = \frac{1}{x^2+y^2}(x, -y) = \frac{1}{|z|^2}\bar{z}$, where $\bar{z} = (x, -y)$, so that $z^{-1} * z = \frac{z\bar{z}}{|z|^2} = 1$.

Example 4. Consider the 2-dimensional subspace of the 4-dimensional real vector space

$$M = \{z = (x, -y, y, x) | x, y \in \mathbb{R}\} \subset \mathbb{R}^4$$

and introduce the componentwise addition (translation) and the new multiplication $\times$ for $z_j = (x_j, -y_j, y_j, x_j), j = 1,2$

$$z_1 \times z_2 = (x_1 x_2 - y_1 y_2, -(x_1 y_2 + x_2 y_1), x_1 y_2 + x_2 y_1, x_1 x_2 - y_1 y_2). \tag{2.6}$$

Then $(M, +,\times)$ forms a field isomorphic to $\mathbb{C}$.

Let $\mathbb{R}[X]$ denote the ring of all polynomials with real coefficients, where the polynomial ring is nothing other than the direct sum $\sum \mathbb{R}$ of infinitely many copies of $\mathbb{R}$(see below).

Example 5. Let j denote a root (in the algebraic closure of $\mathbb{R}$ provided that it exists) of the irreducible polynomial $X^2 + 1$over $\mathbb{R}$, irreducible because for any real number α, $\alpha^2 + 1 > 0$ and $X^2 + 1$ cannot be decomposed into a product of linear factors. The adjoint$\mathbb{R}(j) = \{a + bj | a, b \in \mathbb{R}\}$ is a field, which is seen to be isomorphic to $\mathbb{C}$.

Example 6. Let $\mathbb{R}[X]$ denote the ring of all polynomials with real coefficients, where the polynomial ring is nothing other than the direct sum $\sum \mathbb{R}$ (see below). Let j denote a root of the irreducible polynomial $X^2 + 1$over $\mathbb{R}$, irreducible because for any real number α, $\alpha^{+}1 > 0$ and $X^2 + 1$ cannot be decomposed into a product of linear factors.

The factor ring $\mathbb{R}[X]/(X^2 + 1)$ forms a field which is isomorphic to the adjoint $\mathbb{R}(j) = \{a + bj | a, b \in \mathbb{R}\}$ in Example 5.

Proof. We may directly prove the assertion in Example 6 as follows. Since

$$\mathbb{R}[X]/(X^2 + 1) = \{a + bX \bmod (X^2 + 1) | a, b \in \mathbb{R}\},$$

we may prove that the mapping $a + bX \to a + bj$ is a field isomorphism.

In the multiplication $(a_1 + b_1 X)(a_2 + b_2 X) = a_1 a_2 + b_1 b_2 X^2 + (a_1 b_2 + a_2 b_1)X$, we are to replace $X^2 + 1$ by 0, i.e. X^2 by -1 to obtain $(a_1 + b_1 X)(a_2 + b_2 X) = a_1 a_2 - b_1 b_2 + (a_1 b_2 + a_2 b_1)X$ which corresponds to the operation $(a_1 + b_1 j)(a_2 + b_2 j) = a_1 a_2 + b_1 b_2 j^2 + (a_1 b_2 + a_2 b_1)j$, wherein we are to replace j^2 by -1.

3. Formal Power Series

It often happens that beginners find difficulties in following the argument that in place of code words one considers the corresponding polynomials. The difficulties come from a non-thorough interpretation of cyclic codes as polynomials, which in turn arises from the fact that polynomials are not well understood.

Our objective is to present the concept that the polynomial ring may be thought of as the Cartesian product of infinitely many copies of the ring of scalars with only finitely many non-zero components, whose elements may therefore be written in the form of polynomials.

3.1. Formal Power Series Rings

Let R be a commutative ring with unity 1. In Example 2, we choose the index set to be $\mathbb{N} \cup \{0\}$ (or any countable set, say $\mathbb{N}$). Then the Cartesian product $\prod_{k=0}^{\infty} R = \{c = (c_0, c_1, \cdots) | c_k \in R\}$ of infinitely many copies of R forms a ring under componentwise addition and multiplication with unity.

Let X denote an indeterminate and we view the element $c = (c_0, c_1, \cdots)$ as a formal power series

$$c = c(X) = c_0 + c_1 X + \cdots. \qquad (3.1)$$

The set of all the formal power series over R is denoted by

$$R[[X]] = \{c_0 + c_1 X + c_2 X^2 + \cdots | c_k \in R\} \qquad (3.2)$$

on which there are defined componentwise addition and the new Cauchy product as multiplication: For two formal power series $\alpha(X) = a_0 + a_1 X + a_2 X^2 + \cdots$, we define

$$\begin{aligned} \alpha(X) + \beta(X) &= a_0 + b_0 + (a_1 + b_1)X + \cdots, \\ \alpha(X)\beta(X) &= a_0 b_0 + (a_0 b_1 + a_1 b_0)X + \cdots + c_k X^k + \cdots, \end{aligned} \qquad (3.3)$$

The scalar product by elements of R may be defined as

$$c\alpha(X) = ca_0 + ca_1 X + \cdots. \qquad (3.4)$$

With these operations $R[[X]]$ forms an R-module as well as a ring (i.e. an algebra), called the formal power series ring.

3.2. Polynomial Rings

A polynomial γ is a terminating formal power series, i.e. a sequence with all but finite number of coordinates being 0. Therefore there exits the maximal index $n \in \mathbb{N} \cup \{0\}$ such that $c_n \neq 0,\ c_k = 0, \quad k > n + 1$:

$$\gamma = (c_0, c_1, \cdots, c_n, 0, 0, \cdots), \qquad (3.5)$$

which, correspondingly to (3.1), may be expressed as

$$\gamma = c_0 + c_1 X + c_2 X^2 + \cdots + c_n X^n \qquad (3.6)$$

called a polynomial of degree$n$ (denoted: $\deg \gamma = n$). $c_n$is called the leading coefficient.

3.3. Polynomial Functions

Let S/R be a ring extension and let $f(X) = c_0 + c_1 X + \cdots + c_n X^n \in R[X]$with $c_n \neq 0$. Then for an element $\alpha \in S$, the expression $c_0 + c_1 \alpha + \cdots + c_n \alpha^n$ is an element of S, which we may write $f(\alpha)$ and we call the process of forming $f(\alpha)$ from $f(X)$substitution of α in the variable X with $f(\alpha)$ being called the value of $f(X)$ at α. In particular, if $f(\alpha) = 0$, then α is called a root of f. If we fix $f \in R[X]$ and let $\alpha \in S$ vary, then we obtain a function $f \in \mathcal{F}(S)$, which is called a polynomial function.

Theorem 3.1. (Polynomial function)If R is an integral domain with infinitely many elements, then we may identify the polynomial and the polynomial function.

Cf. Example 7.

The following lemma is the fundamental theorem in finite field theory.

Lemma 3.1. (i) For any prime power $q = p^e$, there exists a unique finite field $\mathbb{F}_q$ with q elements, which is a splitting field of $X^q - X$ and $\mathbb{F}_q^{\times}$ is a cyclic group of order $q - 1$.

(ii) For any $e \in \mathbb{N}$, there exists a unique extension $\mathbb{F}_{q^e}$ of $\mathbb{F}_q$ of degree e. The extension $\mathbb{F}_{q^e}/\mathbb{F}_q$ is a cyclic extension and the Galois group is generated by σ such that $\alpha^\sigma = \alpha^q \quad (\forall \alpha \in \mathbb{F}_{q^e})$.

Example 7. Let p be a prime. Then by Theorem 3.1, (i), the Fermat little theorem holds true:

$$\alpha^{p-1} = 1, 0 \neq \alpha \in \mathrm{GF}(p) = \mathbb{Z}/p\mathbb{Z}, \qquad (3.7)$$

whence $\alpha^p = \alpha$ and so the polynomial function $f(\alpha) = \alpha^p - \alpha$ is a zero map although the polynomial $f(X) = X^p - X$ is a non-zero polynomial of degree p.

Example 8. Let p be a prime. We take up Example 7. By the Fermat little theorem (Theorem 3.1, (i)) we have the decomposition

$$X^{p-1} - 1 = \prod_{0 \neq \alpha \in \mathbb{Z}/p\mathbb{Z}} (X - \alpha) = \prod_{k=0}^{p-1} (X - k). \quad (3.8)$$

Hence comparing the constant term, we obtain

$$(p-1)! \equiv -1 \mod p, \qquad (3.9)$$

which is called Wilson's theorem.

4. Polynomials and Code Words

Our objective in this section is to elucidate somewhat vague situation surrounding the (cyclic) code and the corresponding polynomial. As is shown in §3.2, polynomials are rewriting of the coordinates. But this interpretation does not seem well perceived in engineering disciplines and it happens that beginners find difficulties in following the argument that in place of code words one considers the corresponding polynomials. We elucidate this situation by the following

Definition 2. To each codeword$c = (c_0, c_1, \cdots, c_{n-1}) \in F^q$, by the very definition, there corresponds the polynomial $c(X) = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}$ called the code polynomial and we identify them. We also write $p_c(X) = (c_{n-1}, c_1, \cdots, c_0) = c_{n-1} + c_0 X + \cdots + c_{n-2} X^{n-1}$, which is the representor $p_c(X)$.

This clarifies the setting in many papers including [6], [11], [12], etc.

5. Cyclic Codes

In this section we present the theory of cyclic codes in the language of polynomials $(\mathrm{GF}(q)[X]/(X^n - 1))$. In the first subsection we appeal to the structure theorem of the factor ring of the polynomial ring over a field modulo a polynomial to the effect that it is a PID and such is the factor ring. Here we need the notion of equivalence classes in addition to that of polynomials or Cartesian products.

5.1. Argument Depending on the PID Structure

In this subsection we need the following facts.

Theorem 5.1. (Euclidean division)The polynomial ring over an integral domain is a Euclidean ring. More concretely, let $f, g \in R[X]$ and let the leading coefficient of g lies in $R^{\times}$. Then there exist polynomials $r, q \in R[X]$ such that

$$f(X) = g(X)q(X) + r(X) \tag{5.1}$$

with $deg\, r < deg\, g$. If R is an integral domain, then q, r are uniquely determined.

Theorem 5.2. (Euclidean → PID → UFD)A Euclidean domain is a principal ideal domain (PID). A PID is a unique factorization domain (UFD). Hence a Euclidean domain is UFD, and a fortiori, the polynomial ring is a UFD.

Definition 3. Let C be a linear code $\subset GF(q)^n$. If for any of its element $\boldsymbol{c}$,

$$\begin{aligned} \boldsymbol{c} = (c_0, c_1, \cdots, c_{n-1}) \in C \\ \Rightarrow p(\boldsymbol{c}) := (c_{n-1}, c_0, \cdots, c_{n-1}) \in C \end{aligned} \tag{5.2}$$

holds (hence all shifts belong to C by induction), then C is called acyclic code.

Example 9. (i)

$$C_1 = \{(0,0,0), (1,1,0), (1,0,1), (0,1,1)\} \tag{5.3}$$

is a cyclic code.

(ii) Let C_2 be a binary linear code given by its parity check matrix

$$H_2 = \begin{pmatrix} 1011100(19) \\ 1110010(20) \\ 0111001(21) \end{pmatrix} = (-{}^tA, I). \tag{5.4}$$

The generating matrix G_2 for C_2 is seen to be

$$G_2 = \begin{pmatrix} 1000110(23) \\ 0100011(24) \\ 0010111(25) \\ 0001101(26) \end{pmatrix}, \tag{5.5}$$

It is well-known that the theory of cyclic codes can be described most clearly in terms of the polynomials (or more naturally, we identify a codeword with its code polynomial; cf. Theorem 5.3). Hereafter we let F be a field (finite or not) and let $F[X]$ denote the ring of all the polynomials with coefficients in F, with X an indeterminate. However, whenever we speak of codes, the field is to be thought as finite: $F = \mathbb{F}_q$. Some basic notions needed to follow the subsequent argument may be found in [10, §1.5], which also serves as a source for preceding sections. The main ingredient is Theorem 5.2 to the effect that a polynomial ring over a field is a PID, which entails the following

Proposition 5.1. Let $m = m(X)$ be a non-zero polynomial in $F[X]$ with coefficients in a field F. Then the factor ring $F[X]/(m(X)) = \{\bar{f} | f = f(X) \in F[X]\}$ is a PID. Moreover, it is generated by a divisor $h = h(X)$ of $m(X)$: $F[X]/(m(X)) = (\overline{h(X)})$, where $h(X)$ may be chosen to be monic.

Proof. Let $\mathfrak{i}$ be an ideal of $F[X]/(m(X))$. Let $\mathfrak{j} = \{f(X) \in f[X] | \bar{f} \in \mathfrak{i}\}$. Then we may show that $\mathfrak{j}$ is an ideal of $F[X]$. Hence it must be a principal ideal, say $\mathfrak{j} = (h(X))$ with a polynomial $h(X) \in F[X]$. Then clearly $\mathfrak{i} = (\bar{h})$.

Note that since $\overline{m(X)} = \bar{0} \in \mathfrak{i}$, it follows that $m(X)$ is divisible by $h(X)$, i.e. h is a divisor of m. If the leading coefficient of $h(X)$is $c_m \neq 0$, then we may use $c_m^{-1} h(X)$ as a generator of $F[X]/(m(X))$.

Proposition 5.2. In the factor ring $F[X]/(m(X))$, where $deg\, m = n \geq 1$, a complete set of residues is given by the residues modulo $m(X)$:

$$\begin{aligned} F[X]/(m(X)) &= \{\overline{r(X)} | r(X) \in F[X], \deg r < n\} \\ &= \{\overline{c_c + c_1 X + \cdots + c_{n-1} X^{n-1}} | c_i \in F\}. \end{aligned} \tag{5.6}$$

Proof. For any polynomial $f = f(X)$, we have by the Euclidean algorithm,

$$f = mq + r, \quad q, r \in F[X], \quad \deg r < n, \tag{5.7}$$

whence $\bar{f} = \bar{r}$. Further, if $\deg r < n, \deg s < n$, then $\deg(r - s) < n$, and so $r - s \notin (m)$. Hence $\bar{r} \neq \bar{s}$. Hence the given set is a complete set of residues modulo $m(X)$.

Definition 4. For each codeword$c = (c_0, c_1, \cdots, c_{n-1}) \in F^q$, we correspond the polynomial $c(X) = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}$ called thecode polynomialand we identify them. We also write $p_c(X) = (c_{n-1}, c_1, \cdots, c_0) = c_{n-1} + c_0 X + \cdots + c_{n-2} X^{n-1}$, which is the representor.

Theorem 5.3. In Definition 2, we may identify the codeword and the code polynomial by the embedding

$$f : C \to F[X]; \; f((c_0, c_1, \cdots, c_{n-1})) = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}. \tag{5.8}$$

Proof. With the Cauchy product (3.3), the polynomials form a ring. The mapping in (5.8) is a linear monomorphism and so C may be identified with its image $f(C) = \{c_0 + c_1 X + \cdots + c_{n-1} X^{n-1} | c_i \in F\}$.

Lemma 1. We have

$$p_{\boldsymbol{c}}(X) = X\boldsymbol{c}(X) - c_{n-1}(X^n - 1) \equiv X\boldsymbol{c}(X) \bmod (X^n - 1). \tag{5.9}$$

This Lemma motivates one to consider the factor ring $F[X]/(X^n - 1)$ whose elements are $\overline{c(X)} = \overline{c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}}$. Lemma 1 means

$$\bar{X} \overline{c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}} = \overline{c_{n-1} + c_0 X + \cdots + c_{n-2} X^{n-1}},$$

where the right-hand side corresponds to the shift $(c_{n-1}, c_0, \cdots, c_{n-2})$. By induction, we have

$$\begin{aligned} &\overline{X^j}\, \overline{c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}} \\ &\qquad = \overline{c_{n-j} + c_{n-j+1} X + \cdots + c_{n-j-1} X^{n-1}}, \end{aligned}$$

which corresponds to the jth shift. Hence if all these residue classes belong to C, then C is a cyclic code.

The following two theorems are fundamental in the theory of cyclic codes.

Theorem 5.4. Suppose C is a linear code $\subset F^n$ and let

$$\mathfrak{i} = \{\overline{\boldsymbol{c}(X)} | \boldsymbol{c} \in C\}.$$

Then C is a cyclic code if and only if $\mathfrak{i}$ is an ideal of $F[X]/(X^n - 1)$.

Proof. Suppose C is a cyclic code and let $c = (c_0, c_1, \cdots, c_{n-1})$,

$c' = (c_0{}', c_1{}', \cdots, c_{n-1}{}')$ be arbitrary codewords. Then $\overline{c(X)} \pm \overline{c'(X)}$ corresponds to $\boldsymbol{c} \pm \boldsymbol{c}'$, so that the sum and difference belong to C. For any $a \in F$, the polynomial $\bar{a}\overline{\boldsymbol{c}(X)}$ corresponds to $a\boldsymbol{c}$. By Lemma 5.1, for any power of X, we have $\overline{X^j}\,\overline{\boldsymbol{c}(X)} \in C$. Hence for any element $a(X) \in F[X]$, we have $\overline{a(X)}\,\overline{\boldsymbol{c}(X)} \in \mathfrak{i}$. Hence $\mathfrak{i}$ is an ideal of $F[X]/(X^n - 1)$.

Conversely, if $\mathfrak{i}$ is an ideal of $F[X]/(X^n - 1)$, then for any $\boldsymbol{c}(X) \in C$, we have $\bar{X}\overline{\boldsymbol{c}(X)} \in C$, which means that that the shift $(c_{n-1}, c_0, \cdots, c_{n-2}) \in C$ and hence all the shifts also belong to C, which means that C is a cyclic code.

Theorem 5.5. If a linear code $C \subset F^n$ is a cyclic code, then there exists a unique monic divisor $g = g(X)$ of $X^n - 1$ such that

$$C = \{c \in F^n | c(X) \text{ is a multiple of } g(X)\}. \tag{5.10}$$

Conversely, if there is such a g, then C is a cyclic code. Moreover, we have

$$\dim\ _F C + \deg g = n. \tag{5.11}$$

Proof. If C is a cyclic code, then the set $\mathfrak{i}$ in Theorem 5.4 is an ideal, which in view of Proposition 5.1, must be principal, say $\mathfrak{i} = (g(X))$ with a monic $g(X) \in F[X]$ which is a divisor of $X^n - 1$. Hence C is given as (5.10).

We turn to the proof of (5.11). Let $\deg g = s$. Recall Proposition 5.2 giving a complete set of residues modulo $X^n - 1$. Then we see that for $\boldsymbol{c}$ belongs to C, it is necessary and sufficient that

$$\overline{\boldsymbol{c}(X)} = \overline{g(X)}\,\overline{q(X)}, \tag{5.12}$$

where $\deg q < n - m$. I.e. that $\boldsymbol{c}(X) = g(X)r(X)$ with $r(X) = c_0 + c_1X + \cdots + c_{n-m-1}X^{n-m-1}$. Since there are q^{n-s} choices for the coefficients c_i', we have $\# C = q^{n-s}$. I.e. (5.11) holds true.

Conversely, if there is a g for which (5.10) holds true, then the set $\mathfrak{i}$ in Theorem 5.4 is $(g(X))$, a principal ideal. Hence by Theorem 5.4, C is a cyclic code.

Definition 5. The unique polynomial $g(X) | (X^n - 1)$ given in (5.10) is called agenerating polynomialof the cyclic code C. $C$is then called a cyclic code with the generating polynomial$g$.

Hence, by examining the divisors of $X^n - 1$, we may study the cyclic codes.

Note that the argument given above is an structural counterpart of the argument of [7]. In the latter, a more constructive and elementary way is adopted relying on the existence of the minimal polynomial.

6. PSO

PSO, Particle Swarm Optimization, is a biologically-inspired stochastic optimization technique arising from the family of evolutionary computation and gives better solutions than GA (Genetic Algorithm). In the original version of PSO due to Kennedy and Eberhart [15], a swarm consists of N particles moving around a prescribed D-dimensional search space. The i-th particle is denoted by $X_i = (x_{i1}, \cdots, x_{iD})$, $1 \le i \le N$ whose best previous solution (*pbest*) is denoted by $P_i = (p_{i1}, \cdots, p_{iD})$, while the best solution (*gbest*) achieved by the whole swarm is denoted by $P_g = \left(p_{g1}, \cdots, p_{gD}\right)$. The current velocity (rate of change of its position) of the i-th particle is denoted by $V_i = (v_{i1}, \cdots, v_{iD})$.

At each step, each particle moves toward the *pbest* and *gbest* locations. In the improved PSO, particles are manipulated by the following equations

$$\begin{aligned} v_{id}(k+1) &= wv_{id}(k) + c_1\Re_1(p_{id} - x_{id}(k)) \\ &\qquad + c_2\Re_2\left(p_{gd} - x_{id}\right), \\ x_{id}(k+1) &= (1 - mc)x_{id}(k) + mcv_{id}(k+1), \\ &1 \le i \le N,\ 1 \le d \le D, \end{aligned} \tag{6.1}$$

where c_1 resp. c_2 are positive constants called cognitive learning rate resp. social learning rate, w is a time decreasing inertia factor (weight), $rand$ is a random function with values in [0,1], and mc is a momentum factor. The velocity of the particles is limited to $[V_{\min}, V_{\max}]$ and $V_{\min} = X_{\min}, V_{\max} = X_{\max}$.

In [4], fractional calculus which can provide traditional PIDs with a novel and higher performance at the sacrifice of increased complexities arising from specifications of the 5 parameters including integral and derivative orders. An intelligent optimization method can be used for designing it which make use of PSO.

A swarm is the battery stack consisting of $N = 180 \sim 216$ particles and a particle searches in the $\mathbb{R}^D$ with $D = 36$ for its best position $3.6V$. A typical block of cells is a series (cascade) connection of 12 cells combined as a 3 parallel array: $3P12S$.

The i -th particle is denoted by $x_k(t) = \left(x_{k1}(t), \cdots, x_{kD}(t)\right), 1 \le k \le N$, and $x_{kd}(t)$ indicates the amount of charge at time t. The velocity of each particle is the charging time to its full load. As in [23], at the battery screening test, the minimum charging time will become known and it is the value of the $V_{\min} = T_{\text{ch}}^i$ in [23].

We consider the stochastic process

$$x_i(k+1) = (1 - mc)x_i(k) + mcv_i(k+1), \tag{6.2}$$

or

$$x_i(k+1) = (1 - mc - \Lambda_1\Re_1 - \Lambda_2\Re_2x_i(k) + (mc + w)v_i(k+1) + C_i, \tag{6.3}$$

where

$$C_i = \Lambda_1 \Re_1 P_{best,i} - \Lambda_2 \Re_2 G_{best}.$$

6.1. Nested PSO

In the problem considered by us, we have a stack of 5-8 blocks of batteries connected in series. Hence these blocks will in turn be the particles in our swarm. The problem here is that the position and the velocity of each block is not known. The block consists of 3-4 parallel arrays of a connection of 12 cells connected in series. Now the position values of these cells inside a block define the position vector of the block and their individual position values are itself governed by the PSO algorithm in the swarm of cells. Thus basically the PSO algorithm has been nested here. First we need to apply the algorithm for the cells connected in series inside a block so as to be able to define the position vector for the block. When we have the position vector of the components of the block, then we apply the algorithm on the block with these values of the position of its constituents.

Theorem 6.1. (A speculation) Homeostasis –chemo -dynamical stability after replication of cells as well as PSO algorithms may be though of as nested Cartesian product under suitable interpretation of the stochasticity.

6.2. Optimization Criteria and a Fitness Function

Two optimization criteria are often used ITAE and ISE, which are short-hands for *integral of time-weighted absolute error* and *integral of squared error*:

$$J_1 = \int_0^\infty |\, e(t)|\, \mathrm{d}t, \quad J_2 = \int_0^\infty |e(t)|^2 \; \mathrm{d}t. \qquad (6.4)$$

The finite part of these mean values is a link that connects control theory and number theory, in the latter of which an essential role is often played by the mean square estimate, i.e. an asymptotic behavior of the finite part $J_2(x) = \int_0^x |e(t)|^2 \; \mathrm{d}t$. Cf. also [22] for finite power signals. J_1 is feasible to good response but its selection performance is not good, while J_2 can track errors quickly but easily lead to oscillation. In [4], [24], the weighted combination of ITAE and the (square of) control input:

$$J = \int_0^\infty (w_1 |e(t)| + w_2 u^2(t)) \; \mathrm{d}t, \qquad (6.5)$$

where $0 < w_i < 1$ ($w_1 = 0.99, w_2 = 0.001$ is used). Then the fitness function is $1/J$.

References

[1] R. C. Blei, Fractional Cartesian products of sets, Ann. Inst. Fourier (Grenoble) 29 (1979), 79-105.

[2] C. Bonfiglio and W. Roessler, A cost optimized battery management system with active cell balancing for Lithium ion battery stacks, IEEE 2009.

[3] A. Carbone and M. Gromov, A mathematical slices of molecular biology, Supplement to volume 88 of Gazette des Mathématiciens, French Math. Soc. (SMF), Paris 2001?

[4] J. -Y. Cao and B. -G. Cao, Design of fractional order controllers based on particle swarm optimization, 2006.

[5] P. J. Davis and R. Hersh, Descartes' dream—The world according to mathematics, Harcourt Brace Jovanovich Publ., San Diego etc. 1986.

[6] L. Jiang, S. Kanemitsu and H. Kitajima, Circulants, linear recurrences and codes, Ann. Univ. Sci. Budapest. Eötvös Sect. Comput.,to appear.

[7] J. Justesen and T. Hoholdt, A course in error correcting codes, European Math. Soc. 2004.

[8] S. Kanemitsu and M. Waldschmidt, Matrices of finite Abelian groups, finite Fourier transforms and codes, Proc. 6th China-Japan Sem. Number Theory, World Sci. London-Singapore-New Jersey, 2013, 90-106.

[9] J. Kotre, White gloves—How we create ourselves from our memory, The Free Press, New York etc. 1995.

[10] [NTA] F.-H. Li, N.-L. Wang and S. Kanemitsu, *Number Theory and its Applications*, World Scientific, Singapore etc. 2013.

[11] J. L. Massey, Shift-register synthesis and BCH decoding, IEEE Trans. on Info. Th. IT-15 (1969), 122-127.

[12] J. L. Massey, The discrete Fourier transform in coding and cryptography, IEEE Inform. Theory Workshop ITW 98, San Diego (1998), 9-11.

[13] Y. Hayakawa, Systems and their control, Ohmsha, Tokyo 2008 (in Japanese).

[14] J. W. Helon and O. Merino, Classical control using H^∞ method, Theory, optimization, and design, SIAM. Philadelphia 1998.

[15] J. Kennedy and R. C. Eberhart, Particle swarm optimization, Proc. IEEE Intern. Conf. Neural Networks, 1942-1948, Piscateway, New Jersey 1995.

[16] H. Kimura, Chain scattering approach to H^∞ -control, Birkhäuser, Boston/Basel/Berlin 1997.

[17] I. Podlubny, Fractional-order systems and $PI^\lambda D^\delta$ controllers, IEEE Trans. Autom. Control, 44, No.1 (1999), 208-213.

[18] I. Podlubny, Geometric and physical interpretation of fractional integration and fraction differentiation, Fractional calculus and applied analysis, 5, No. 4 (2002), 367-386.

[19] V.Pless, Introduction to the Theory of Error-Correcting Codes, 2nd ed., Wiley, New York etc.1989.

[20] R. Shoenheimer, The dynamic state of body constituents, Harvard Univ. Press. Massachusetts, 1942.

[21] K. Takahashi, G. Hirano, T. Kaida, S. Kanemitsu, H. Tsukada and T. Matsuzaki, Record of the second and the third interdisciplinary seminars, Kayanomori 14 (2011), 64-72.

[22] K. Takahashi, G. Hirano, T. Kaida, S. Kanemitsu, H. Tsukada and T. Matsuzaki, Fluctuations in science and music, Kayanomori 25 (2014), to appear.

[23] Sh.-Ch. Wang and Y.-H. Liu, PSO-based Fuzzy logic optimization of dual performance characteristic indices for fast charging of Lithium-ion batteries, MS.

[24] Z.-Y. Zou, PSO optimization for cell-balancing charge of Lithium ion batteries, MS.