

Neural Response

Akash K Singh, PhD

IBM Corporation Sacramento, USA

Abstract

The development of interfaces that link the human nervous system with robotic devices or man-made devices has been a main area of research for several groups in the world. These groups focus on the restoration of motor and sensory function to those with degenerative diseases, injury or in amputees. A key component in these systems is a fast, intuitive, bidirectional interface between the biological and mechatronic systems that allows the robotic limb to be controlled as if it were a natural part of the body. Current hand prostheses use electromyographic (EMG) signals, but are limited to a small number of channels and to sensing volition. To achieve sensory feedback and a higher number of control channels, a neuroprosthetic interface are required. In the present study, thin-film longitudinal intra-fascicular electrodes (tLIFE) were implanted in the sciatic nerve of the rabbit. Various sensory stimuli were applied to the hind limb of the rabbit and the elicited signals were recorded using the tLIFEs. These signals were processed to determine whether the different modes of information could be decoded. Signals were Kalman filtered, wavelet denoised, and spike sorted. The classes of spikes found were then used to infer the stimulus applied to the rabbit. Although the signals acquired from a single tLIFE gave poor stimulus recognition, the combination of the signals from multiple sites led to better results. The spike sorting algorithm is also helped by the use of temporal correlation between the channels. A direct outcome of the results is the possibility of increasing the number of channels of control possible with a prosthetic limb.

Keywords- ENG signal, spike sorting, hybrid bionic systems, neuroprostheses.

I. INTRODUCTION

The possibility of controlling an artificial limb by means of biological signals has always fascinated the human beings. In recent years, the development of interfaces that link the human nervous system with robotic artefacts has been the main research topic of several groups in the world [1]–[7]. The goal is the restoration of motor and sensory functions in patients with degenerative diseases and in amputees. Another possible future application is augmentation of able-bodied people.

A. Hand prosthesis control

In order to make the user feel the robotic hand in a natural way, a fast, intuitive, bi-directional flow of information between the nervous system of the user and the smart robotic limb must be established. Presently, this is limited by the interface between the biological and the mechatronic sides. Available hand prostheses use electromyographic (EMG) signals acquired with surface electrodes to let the user select different grasping tasks [8]. Despite the use of this approach, which has advantages as robustness, simplicity to implement, and non-invasiveness, EMG control has several limitations. Chief among these is the failure of making the arm feel a natural part of the body, limited number of channels of control, and the limitation to volition detection. These limitations become a significant with the development of more dexterous prosthetic arms with built in sensors [9]. This is the rationale of the recent attempts to directly connect the peripheral nervous system (PNS) or the central nervous system (CNS) with the artificial device by using invasive neural interfaces. Invasiveness is obviously considered a drawback and is acceptable only if it can lead to significant improvements. While some research groups (e.g., [3]) have focused their activities on invasive interfaces with the CNS, others (e.g., [1], [7]) argue that open issues have to be investigated before considering the possibility of implanting electrodes in the primary cortex. The main arguments are: cortical interfaces are still not acceptable at present stage for hand prostheses application because of their limited robustness; the direct stimulation of the primary sensory cortex S-I in order to elicit sensory feedback, can provoke parallel effects like activation of undesired areas or muscle contraction (see for example [10], [11]).

B. Invasive PNS neural interfaces

Cuff electrodes proved to be robust and reliable. Their low invasiveness is an asset but is also a limitation to the selectivity even though multisite cuff electrodes led to interesting results [12]. Regenerative electrodes are very appealing for the development of hybrid bionic systems but there are still important issues to be addressed from a neurological point of view, and are only justifiable for severed nerves [13]. Intra-neural multielectrode arrays (MEAs) are capable of selectively recording single unit responses and allow low-current high-selective stimulation of motoneurons. But the limited number of active electrodes and high invasiveness, and their rigid structures should be

taken into account when choosing a neural interface. Generally, low invasive extraneural electrodes (such as cuff and epineurial) have reduced selectivity because they give simultaneous interface to an ensemble of axons in the nerve, while more invasive intrafascicular, penetrating and regenerative electrodes are more selective and allow interaction with small groups of axons within a nerve fascicle. In this scenario Longitudinal Intra-Fascicular Electrodes (LIFEs) could be a nice trade-off thanks to a reduced (although not absent) invasiveness and a good selectivity.

C. LIFE electrodes

LIFEs are constructed from thin insulated conducting wires (such as Pt-Ir or metallized Kevlar fibers) inserted longitudinally into the nerve [14], [15]. They lie in-between and parallel to the nerve fibers gathering signals from only a small number of them. This allows more selective recordings than, e.g., cuff electrodes, that wrap the whole nerve measuring the combined activity of all axons in the nerve. On the other hand LIFE electrodes are less invasive than intraneural multielectrode arrays that are inserted transversally into the nerve leading to a high risk of nerve damage. A recently found problem with LIFEs is that the recording active sites of the electrodes can drift out of measuring distance of the nerve fascicle. Actuated LIFEs are under study in order to “follow” the signal [16]. Recently thin film LIFEs (tLIFE or tfLIFE) have been developed [17]. tfLIFEs allow multi-unit peripheral nerve recordings with 8 recording pads. The substrate for the electrode is made out of photosensitive polyimide because of its biocompatibility, flexibility and structural properties. This substrate filament is folded in half such that each side hosts 4 active recording sites. A tungsten needle is used for implanting the electrode and then removed after insertion. Often signals recorded using different neural interfaces have been used to pick up useful sensory information to enhance the performance of Functional Electrical Stimulation (FES) systems. Recently, the use of LIFE electrodes for the control of a hand prosthesis has been investigated [18]. By means of electrodes implanted in nerve stumps, amputees were able to control one coordinate of a cursor on a PC screen. It was also possible to give the user sensory feedback through stimulation of afferent nerves. This shows that electroneurographic (ENG) interfaces are bidirectional and allow more than a simple binary control. In this study we investigated the possibility of using one single electrode to distinguish spikes from different afferent nerve fibers in order to discriminate different stimuli applied to the paw of a rabbit. This could represent a preliminary step before experiments with human subjects to verify whether the number of commands per electrode the user can send to the robotic arm can be increased.

II. METHODS

A. Animal preparation

The experimental procedures were approved by the Danish Committee for the Ethical Use of Animals in Research. An 8-9 months old female New Zealand White rabbit (4.2 kg) was anaesthetized using a Hypnorm/Dormacrom cocktail (0.15 mg/kg Midazolam (DormicumTM, Alpharma A/S, Norway), 0.03 mg/kg Fentanyl and 1 mg/kg Flurazepam combined in HypnormTM, Janssen Pharmaceutica, Belgium) administered intramuscularly every 20 minutes. The left leg was shaved and the skin overlying the lateral surface of thigh was sprayed with XylocaineTM(lidocaine) prior to opening the skin to provide topical anaesthesia of the skin. A lateral access was created above the popliteal fossa for implanting LIFEs. The popliteal fat pad was removed to allow access to the branches of the sciatic nerve, which branch at the popliteal fossa. The medial gastrocnemius nerve and lateral gastrocnemius/soleus nerves were identified by visual inspection, and by tracing the nerve to the muscle. Two tfLIFE have been implanted (LIFE1 electrode 1A30, LIFE2 electrode 1A14) in the sciatic nerve and a tripolar cuff electrode placed proximally to the LIFEs. All sites of the electrodes got in the nerve.

B. Stimulation

The experiment session consisted of several protocols. In the protocol relevant to this paper different kinds of stimuli were applied to the paw of the rabbit:

- Squeezing the foot with knee at 90°;
- Squeezing the foot with knee released;
- Ankle flexion;
- Toe extension;
- Toe extension combined with ankle flexion.

Each was repeated 4 to 6 times

C. ENG signal acquisition

Signals were amplified by using an 8 channel custom built low-noise headstage amplifier. It has a gain of 1000x, high-pass filter at 0.1 Hz and an input impedance of approx. 10 MΩ. The recording chain following the amplifier consisted of an Axon Cyberamp 380 which high-pass filtered the data at 1 Hz, removed any residual DC offset and post-amplified the signal obtaining a complex gain of 2500x. The signals were then acquired by a customized Alexis XT 16 bit digital tape recorder (gain 1/3) at the sampling rate of 48 kHz. In the part of the experiment relevant to this paper electrodes 1, 2, 3, 4 of the B-side of the tfLIFE were recorded.

D. Signal preprocessing

1) **Downsampling:** Data acquired at 48 kHz were later downsampled to 12 kHz using “sox”, a

multiplatform utility for audio files conversion. The algorithm used is a polyphase interpolation with Nuttall (~ 90 dB stopband) window and approximate filter length of 1024 samples.

2) **Kalman filter:** Signals are later processed with a Kalman filter implemented in C. The noise covariance R for the filter is set to an estimation of the noise variance found as square of the median of the signal multiplied by 0.6745 (this equals the standard deviation for normally distributed data). The process noise covariance Q was fixed at the value 10⁻³.

3) **Wavelet denoising:** Signals underwent a wavelet denoising implemented in C. Using Dyadic Wavelet Decomposition the signal is split in “detail” and “approximation” using the mother wavelet Symlet 7. DWT is recursively applied to the approximation up to the 5th level of decomposition. Detail coefficients of all levels are set to zero if their absolute value does not reach a threshold (hard thresholding method) where θ is proportional to an estimation of the standard deviation of the coefficients at that level. This estimation is carried out by using the median of the absolute value. The inverse process of the DWT, the IDWT, is then performed by using the thresholded details and approximation. The resulting signal is a denoised version of the original one.

E. Spike Sorting

In order to improve selectivity a spike sort algorithm is implemented. In general, this is possible because action potentials gathered from the electrode have different shapes depending on the type of the neuron, its distance from the recording site, and the electrical characteristics of the tissues in between. The approach followed is derived from [19], [20]. A threshold is used to detect spikes. If a sample of the denoised signal is greater than this threshold a time window starting 6 samples before and lasting 9 samples after is extracted. The window length, 16 samples at 12 kHz, correspond to ~ 1.3 ms. In order to distinguish different spike classes from a single signal, a spike sorting algorithm has been used. It consists in a two phase process. During the first phase a set of spike templates is created. During the second phase these templates are used to classify the spikes in the signal.

1) **Templates creation:** If the extracted spike is similar to any class template present in the set, the corresponding template is updated taking into account the new, element otherwise a new class is created. To assess similarity between the spike and the template, the spike is first aligned to the template using the lag that maximizes the crosscorrelation, then two criteria must be satisfied:

- the correlation coefficient between the two must be greater than 0.9;

- the ratio between the mean square difference of the two and the power of the template must be less than 0.5.

If the spike meets these criteria, it is included in the class. The template is updated as the weighted average of the spike and the template using as weight the number of spikes the class contains. To reject artefacts or non-significative classes, very small ones are removed if they have no new spike joining it after a certain time. At the end of the process an xml file with all the definitive class templates is saved for later usage.

2) **Templates matching:** The second pass is identical to

the first one with the exception that class templates found in the first phase are not updated. Every spike is annotated with the number of the class it belongs to.

III. MICROFABRICATION METHODS

Different kinds of microtechnology were used to fabricate electrodes for neuroprosthetics applications. The two mainly used technologies are the production of thinfilm structures and the use of silicon needles. Additionally, microtechnologies like microassembling encapsulation techniques are developed to upgrade the electrodes to active neural implants. Depending on the application, functional encapsulation and implantation tools were developed. Samples of electrodes that were fabricated with the technology described above are cuff, shaft, sieve, intrafascicular and needle electrodes [12].

A. Channel combination

To assess whether different kinds of stimuli could be discriminated from one single channel, we used the percentages of spikes belonging to each class as features. The desired behaviour was that different stimuli would have significantly different preferred spike classes. The result was not as good as expected and we decided to combine information from different recording sites of the tfLIFE electrode. The acquired data contained recordings from electrodes 1 to 4, side B of tfLIFE. The combinations were chosen so that the vector w of the weights of the four channels had unitary norm and every component could have 9 different values in [1, 1] giving an equispaced hyperspherical grid of points. At the same time it should favour similar percentages for stimuli of the same type. We used where σ_2 is the inter-stimuli variance, i.e. the variance of the average percentages of each stimuli type, and σ_1 is the intra-stimuli variance, i.e. the average of the variances of stimuli of the same type. To assess the performance of every combination three indices were extracted from every class: the best one (fw), the average of the best three (3fw) and the overall average (fw).

We consider the following anycast field equations defined over an open bounded piece of network and /or feature space $\Omega \subset R^d$. They describe the dynamics of the mean anycast of each of p node populations.

$$\begin{cases} \left(\frac{d}{dt} + l_i\right)V_i(t, r) = \sum_{j=1}^p \int_{\Omega} J_{ij}(r, \bar{r}) S[(V_j(t - \tau_{ij}(r, \bar{r}), \bar{r}) - h_{ij})] d\bar{r} \\ \quad + I_i^{ext}(r, t), \quad t \geq 0, 1 \leq i \leq p, \\ V_i(t, r) = \phi_i(t, r) \quad t \in [-T, 0] \end{cases}$$

We give an interpretation of the various parameters and functions that appear in (1), Ω is finite piece of nodes and/or feature space and is represented as an open bounded set of R^d . The vector r and \bar{r} represent points in Ω . The function $S: R \rightarrow (0, 1)$ is the normalized sigmoid function:

$$S(z) = \frac{1}{1 + e^{-z}} \quad (2)$$

It describes the relation between the input rate v_i of population i as a function of the packets potential, for example, $V_i = v_i = S[\sigma_i(V_i - h_i)]$. We note V the p - dimensional vector (V_1, \dots, V_p) . The p function $\phi_i, i = 1, \dots, p$, represent the initial conditions, see below. We note ϕ the p - dimensional vector (ϕ_1, \dots, ϕ_p) . The p function $I_i^{ext}, i = 1, \dots, p$, represent external factors from other network areas. We note I^{ext} the p - dimensional vector $(I_1^{ext}, \dots, I_p^{ext})$. The $p \times p$ matrix of functions $J = \{J_{ij}\}_{i,j=1,\dots,p}$ represents the connectivity between populations i and j , see below. The p real values $h_i, i = 1, \dots, p$, determine the threshold of activity for each population, that is, the value of the nodes potential corresponding to 50% of the maximal activity. The p real positive values $\sigma_i, i = 1, \dots, p$, determine the slopes of the sigmoids at the origin. Finally the p real positive values $l_i, i = 1, \dots, p$, determine the speed at which each anycast node potential decreases exponentially toward its real value. We also introduce the function $S: R^p \rightarrow R^p$, defined by $S(x) = [S(\sigma_1(x_1 - h_1)), \dots, S(\sigma_p(x_p - h_p))]$, and the diagonal $p \times p$ matrix $L_0 = \text{diag}(l_1, \dots, l_p)$. Is the intrinsic dynamics of the population given by the linear response of data transfer. $(\frac{d}{dt} + l_i)$ is

replaced by $(\frac{d}{dt} + l_i)^2$ to use the alpha function

response. We use $(\frac{d}{dt} + l_i)$ for simplicity although

our analysis applies to more general intrinsic dynamics. For the sake, of generality, the propagation delays are not assumed to be identical for all populations, hence they are described by a matrix $\tau(r, \bar{r})$ whose element $\tau_{ij}(r, \bar{r})$ is the propagation delay between population j at \bar{r} and population i at r . The reason for this assumption is that it is still unclear from anycast if propagation delays are independent of the populations. We assume for technical reasons that τ is continuous, that is $\tau \in C^0(\bar{\Omega}^2, R_+^{p \times p})$. Moreover packet data indicate that τ is not a symmetric function i.e., $\tau_{ij}(r, \bar{r}) \neq \tau_{ji}(\bar{r}, r)$, thus no assumption is made about this symmetry unless otherwise stated. In order to compute the righthand side of (1), we need to know the node potential factor V on interval $[-T, 0]$. The value of T is obtained by considering the maximal delay:

$$\tau_m = \max_{i,j(r,r \in \Omega \times \Omega)} \tau_{i,j}(r, \bar{r}) \quad (3)$$

Hence we choose $T = \tau_m$

B. Mathematical Framework

A convenient functional setting for the non-delayed packet field equations is to use the space $F = L^2(\Omega, R^p)$ which is a Hilbert space endowed with the usual inner product:

$$\langle V, U \rangle_F = \sum_{i=1}^p \int_{\Omega} V_i(r) U_i(r) dr \quad (1)$$

To give a meaning to (1), we defined the history space $C = C^0([-\tau_m, 0], F)$ with

$\|\phi\| = \sup_{t \in [-\tau_m, 0]} \|\phi(t)\|_F$, which is the Banach phase space associated with equation (3). Using the notation $V_i(\theta) = V(t + \theta), \theta \in [-\tau_m, 0]$, we write (1) as

$$\begin{cases} V(t) = -L_0 V(t) + L_1 S(V_t) + I^{ext}(t), \\ V_0 = \phi \in C, \end{cases} \quad (2)$$

Where

$$\begin{cases} L_1: C \rightarrow F, \\ \phi \rightarrow \int_{\Omega} J(\cdot, \bar{r}) \phi(\bar{r}, -\tau(\cdot, \bar{r})) d\bar{r} \end{cases}$$

Is the linear continuous operator satisfying $\|L_1\| \leq \|J\|_{L^2(\Omega^2, R^{p \times p})}$. Notice that most of the papers on this subject assume Ω infinite, hence requiring $\tau_m = \infty$.

Proposition 1.0 If the following assumptions are satisfied.

1. $J \in L^2(\Omega^2, R^{p \times p})$,
2. The external current $I^{ext} \in C^0(R, F)$,
3. $\tau \in C^0(\overline{\Omega^2}, R_+^{p \times p})$, $\sup_{\Omega^2} \tau \leq \tau_m$.

Then for any $\phi \in C$, there exists a unique solution $V \in C^1([0, \infty), F) \cap C^0([-\tau_m, \infty), F)$ to (3)

Notice that this result gives existence on R_+ , finite-time explosion is impossible for this delayed differential equation. Nevertheless, a particular solution could grow indefinitely, we now prove that this cannot happen.

C. Boundedness of Solutions

A valid model of neural networks should only feature bounded packet node potentials.

Theorem 1.0 All the trajectories are ultimately bounded by the same constant R if $I \equiv \max_{t \in R^+} \|I^{ext}(t)\|_F < \infty$.

Proof : Let us defined $f : R \times C \rightarrow R^+$ as

$$f(t, V_t) \stackrel{def}{=} \left\langle -L_0 V_t(0) + L_1 S(V_t) + I^{ext}(t), V(t) \right\rangle_F = \frac{1}{2} \frac{d \|V\|_F^2}{dt}$$

We note $l = \min_{i=1, \dots, p} l_i$

$$f(t, V_t) \leq -l \|V(t)\|_F^2 + (\sqrt{p|\Omega|} \|J\|_F + I) \|V(t)\|_F$$

Thus, if

$$\|V(t)\|_F \geq 2 \frac{\sqrt{p|\Omega|} \|J\|_F + I \stackrel{def}{=} R, f(t, V_t) \leq -\frac{lR^2 \stackrel{def}{=} -\delta < 0}}{l}$$

Let us show that the open route of F of center 0 and radius R, B_R , is stable under the dynamics of equation. We know that $V(t)$ is defined for all $t \geq 0$ and that $f < 0$ on ∂B_R , the boundary of B_R . We consider three cases for the initial condition V_0 . If $\|V_0\|_C < R$ and set $T = \sup\{t \mid \forall s \in [0, t], V(s) \in \overline{B_R}\}$. Suppose that $T \in R$, then $V(T)$ is defined and belongs to $\overline{B_R}$, the closure of B_R , because $\overline{B_R}$ is closed, in effect to ∂B_R , we also have

$$\frac{d}{dt} \|V\|_F^2 \Big|_{t=T} = f(T, V_T) \leq -\delta < 0 \quad \text{because}$$

$V(T) \in \partial B_R$. Thus we deduce that for $\varepsilon > 0$ and small enough, $V(T + \varepsilon) \in \overline{B_R}$ which contradicts the definition of T . Thus $T \notin R$ and $\overline{B_R}$ is stable.

Because $f < 0$ on $\partial B_R, V(0) \in \partial B_R$ implies that $\forall t > 0, V(t) \in B_R$. Finally we consider the case $V(0) \in \overline{CB_R}$. Suppose that $\forall t > 0, V(t) \notin \overline{B_R}$, then

$$\forall t > 0, \frac{d}{dt} \|V\|_F^2 \leq -2\delta, \quad \text{thus } \|V(t)\|_F \text{ is}$$

monotonically decreasing and reaches the value of R in finite time when $V(t)$ reaches ∂B_R . This contradicts our assumption. Thus

$$\exists T > 0 \mid V(T) \in B_R.$$

Proposition 1.1 : Let s and t be measured simple functions on X . for $E \in \mathcal{M}$, define

$$\phi(E) = \int_E s d\mu \quad (1)$$

Then ϕ is a measure on M .

$$\int_X (s+t) d\mu = \int_X s d\mu + \int_X t d\mu \quad (2)$$

Proof : If s and if E_1, E_2, \dots are disjoint members of M whose union is E , the countable additivity of μ shows that

$$\begin{aligned} \phi(E) &= \sum_{i=1}^n \alpha_i \mu(A_i \cap E) = \sum_{i=1}^n \alpha_i \sum_{r=1}^{\infty} \mu(A_i \cap E_r) \\ &= \sum_{r=1}^{\infty} \sum_{i=1}^n \alpha_i \mu(A_i \cap E_r) = \sum_{r=1}^{\infty} \phi(E_r) \end{aligned}$$

Also, $\phi(\emptyset) = 0$, so that ϕ is not identically ∞ .

Next, let s be as before, let β_1, \dots, β_m be the distinct values of t , and let $B_j = \{x : t(x) = \beta_j\}$ If

$$E_{ij} = A_i \cap B_j, \quad \text{the}$$

$$\int_{E_{ij}} (s+t) d\mu = (\alpha_i + \beta_j) \mu(E_{ij})$$

$$\text{and } \int_{E_{ij}} s d\mu + \int_{E_{ij}} t d\mu = \alpha_i \mu(E_{ij}) + \beta_j \mu(E_{ij})$$

Thus (2) holds with E_{ij} in place of X .

Since X is the disjoint union of the sets E_{ij} ($1 \leq i \leq n, 1 \leq j \leq m$), the first half of our proposition implies that (2) holds.

Theorem 1.1: If K is a compact set in the plane whose complement is connected, if f is a continuous complex function on K which is holomorphic in the interior of K , and if $\varepsilon > 0$, then there exists a polynomial P such that $|f(z) - P(z)| < \varepsilon$ for all $z \in K$. If the interior of K is empty, then part of the hypothesis is vacuously satisfied, and the conclusion holds for every $f \in C(K)$. Note that K need to be connected.

Proof: By Tietze's theorem, f can be extended to a continuous function in the plane, with compact support. We fix one such extension and denote it again by f . For any $\delta > 0$, let $\omega(\delta)$ be the supremum of the numbers $|f(z_2) - f(z_1)|$ where z_1 and z_2 are subject to the condition $|z_2 - z_1| \leq \delta$. Since f is uniformly continuous, we have $\lim_{\delta \rightarrow 0} \omega(\delta) = 0$ (1) From now on,

δ will be fixed. We shall prove that there is a polynomial P such that $|f(z) - P(z)| < 10,000 \omega(\delta)$ ($z \in K$) (2)

By (1), this proves the theorem. Our first objective is the construction of a function $\Phi \in C_c'(R^2)$, such that for all z

$$|f(z) - \Phi(z)| \leq \omega(\delta), \quad (3)$$

$$|(\partial\Phi)(z)| < \frac{2\omega(\delta)}{\delta}, \quad (4)$$

And

$$\Phi(z) = -\frac{1}{\pi} \iint_X \frac{(\partial\Phi)(\zeta)}{\zeta - z} d\zeta d\eta \quad (\zeta = \xi + i\eta), \quad (5)$$

Where X is the set of all points in the support of Φ whose distance from the complement of K does not exceed δ . (Thus X contains no point which is "far within" K .) We construct Φ as the convolution of f with a smoothing function A . Put $a(r) = 0$ if $r > \delta$, put

$$a(r) = \frac{3}{\pi\delta^2} \left(1 - \frac{r^2}{\delta^2}\right)^2 \quad (0 \leq r \leq \delta), \quad (6)$$

And define

$$A(z) = a(|z|) \quad (7)$$

For all complex z . It is clear that $A \in C_c'(R^2)$. We claim that

$$\iint_{R^2} A = 1, \quad (8)$$

$$\iint_{R^2} \partial A = 0, \quad (9)$$

$$\iint_{R^2} |\partial A| = \frac{24}{15\delta} < \frac{2}{\delta}, \quad (10)$$

The constants are so adjusted in (6) that (8) holds. (Compute the integral in polar coordinates), (9) holds simply because A has compact support. To compute (10), express ∂A in polar coordinates, and note that $\frac{\partial A}{\partial \theta} = 0$,

$$\frac{\partial A}{\partial r} = -a',$$

Now define

$$\Phi(z) = \iint_{R^2} f(z - \zeta) A d\zeta d\eta = \iint_{R^2} A(z - \zeta) f(\zeta) d\zeta d\eta \quad (11)$$

Since f and A have compact support, so does Φ . Since

$$\begin{aligned} & \Phi(z) - f(z) \\ &= \iint_{R^2} [f(z - \zeta) - f(z)] A(\zeta) d\zeta d\eta \quad (12) \end{aligned}$$

And $A(\zeta) = 0$ if $|\zeta| > \delta$, (3) follows from (8).

The difference quotients of A converge boundedly to the corresponding partial derivatives, since $A \in C_c'(R^2)$. Hence the last expression in (11) may be differentiated under the integral sign, and we obtain

$$\begin{aligned} (\partial\Phi)(z) &= \iint_{R^2} (\partial A)(z - \zeta) f(\zeta) d\zeta d\eta \\ &= \iint_{R^2} f(z - \zeta) (\partial A)(\zeta) d\zeta d\eta \\ &= \iint_{R^2} [f(z - \zeta) - f(z)] (\partial A)(\zeta) d\zeta d\eta \quad (13) \end{aligned}$$

The last equality depends on (9). Now (10) and (13) give (4). If we write (13) with Φ_x and Φ_y in place of $\partial\Phi$, we see that Φ has continuous partial derivatives, if we can show that $\partial\Phi = 0$ in G , where G is the set of all $z \in K$ whose distance from the complement of K exceeds δ . We shall do this by showing that

$$\Phi(z) = f(z) \quad (z \in G); \quad (14)$$

Note that $\partial f = 0$ in G , since f is holomorphic there. Now if $z \in G$, then $z - \zeta$ is in the interior of K for all ζ with $|\zeta| < \delta$. The mean value property for harmonic functions therefore gives, by the first equation in (11),

$$\begin{aligned} \Phi(z) &= \int_0^\delta a(r) r dr \int_0^{2\pi} f(z - re^{i\theta}) d\theta \\ &= 2\pi f(z) \int_0^\delta a(r) r dr = f(z) \iint_{R^2} A = f(z) \end{aligned} \quad (15)$$

For all $z \in G$, we have now proved (3), (4), and (5) The definition of X shows that X is compact and that X can be covered by finitely many open discs D_1, \dots, D_n , of radius 2δ , whose centers are not in K . Since $S^2 - K$ is connected, the center of each D_j can be joined to ∞ by a polygonal path in $S^2 - K$. It follows that each D_j contains a compact connected set E_j , of diameter at least 2δ , so that $S^2 - E_j$ is connected and so that $K \cap E_j = \emptyset$. with $r = 2\delta$. There are functions $g_j \in H(S^2 - E_j)$ and constants b_j so that the inequalities.

$$|Q_j(\zeta, z)| < \frac{50}{\delta}, \quad (16)$$

$$\left| Q_j(\zeta, z) - \frac{1}{z - \zeta} \right| < \frac{4,000\delta^2}{|z - \zeta|^2} \quad (17)$$

Hold for $z \notin E_j$ and $\zeta \in D_j$, if

$$Q_j(\zeta, z) = g_j(z) + (\zeta - b_j) g_j^2(z) \quad (18)$$

Let Ω be the complement of $E_1 \cup \dots \cup E_n$. Then

Ω is an open set which contains K . Put $X_1 = X \cap D_1$ and

$X_j = (X \cap D_j) - (X_1 \cup \dots \cup X_{j-1})$, for

$2 \leq j \leq n$,

Define

$$R(\zeta, z) = Q_j(\zeta, z) \quad (\zeta \in X_j, z \in \Omega) \quad (19)$$

And

$$F(z) = \frac{1}{\pi} \iint_X (\partial\Phi)(\zeta) R(\zeta, z) d\zeta d\eta \quad (20)$$

($z \in \Omega$)

Since,

$$F(z) = \sum_{j=1}^n \frac{1}{\pi} \iint_{X_j} (\partial\Phi)(\zeta) Q_j(\zeta, z) d\xi d\eta, \quad (21)$$

(18) shows that F is a finite linear combination of the functions g_j and g_j^2 . Hence $F \in H(\Omega)$. By (20), (4), and (5) we have

$$|F(z) - \Phi(z)| < \frac{2\omega(\delta)}{\pi\delta} \iint_X |R(\zeta, z)|$$

$$-\frac{1}{z - \zeta} |d\xi d\eta| \quad (z \in \Omega) \quad (22)$$

Observe that the inequalities (16) and (17) are valid with R in place of Q_j if $\zeta \in X$ and $z \in \Omega$. Now fix $z \in \Omega$, put $\zeta = z + \rho e^{i\theta}$, and estimate the integrand in (22) by (16) if $\rho < 4\delta$, by (17) if $4\delta \leq \rho$. The integral in (22) is then seen to be less than the sum of

$$2\pi \int_0^{4\delta} \left(\frac{50}{\delta} + \frac{1}{\rho} \right) \rho d\rho = 808\pi\delta \quad (23)$$

And

$$2\pi \int_{4\delta}^\infty \frac{4,000\delta^2}{\rho^2} \rho d\rho = 2,000\pi\delta. \quad (24)$$

Hence (22) yields

$$|F(z) - \Phi(z)| < 6,000\omega(\delta) \quad (z \in \Omega) \quad (25)$$

Since $F \in H(\Omega)$, $K \subset \Omega$, and $S^2 - K$ is connected, Runge's theorem shows that F can be uniformly approximated on K by polynomials. Hence (3) and (25) show that (2) can be satisfied. This completes the proof.

Lemma 1.0 : Suppose $f \in C_c'(R^2)$, the space of all continuously differentiable functions in the plane, with compact support. Put

$$\partial = \frac{1}{2} \left(\frac{\partial}{\partial x} + i \frac{\partial}{\partial y} \right) \quad (1)$$

Then the following "Cauchy formula" holds:

$$\begin{aligned} f(z) &= -\frac{1}{\pi} \iint_{R^2} \frac{(\partial f)(\zeta)}{\zeta - z} d\xi d\eta \\ & \quad (\zeta = \xi + i\eta) \end{aligned} \quad (2)$$

Proof: This may be deduced from Green's theorem. However, here is a simple direct proof:

Put $\varphi(r, \theta) = f(z + re^{i\theta})$, $r > 0$, θ real

If $\zeta = z + re^{i\theta}$, the chain rule gives

$$(\partial f)(\zeta) = \frac{1}{2} e^{i\theta} \left[\frac{\partial}{\partial r} + \frac{i}{r} \frac{\partial}{\partial \theta} \right] \varphi(r, \theta) \quad (3)$$

The right side of (2) is therefore equal to the limit, as $\varepsilon \rightarrow 0$, of

$$-\frac{1}{2} \int_\varepsilon^\infty \int_0^{2\pi} \left(\frac{\partial \varphi}{\partial r} + \frac{i}{r} \frac{\partial \varphi}{\partial \theta} \right) d\theta dr \quad (4)$$

For each $r > 0$, φ is periodic in θ , with period 2π . The integral of $\partial\varphi/\partial\theta$ is therefore 0, and (4) becomes

$$-\frac{1}{2\pi} \int_0^{2\pi} d\theta \int_\varepsilon^\infty \frac{\partial\varphi}{\partial r} dr = \frac{1}{2\pi} \int_0^{2\pi} \varphi(\varepsilon, \theta) d\theta$$

As $\varepsilon \rightarrow 0$, $\varphi(\varepsilon, \theta) \rightarrow f(z)$ uniformly. This gives (2)

If $X^\alpha \in a$ and $X^\beta \in k[X_1, \dots, X_n]$, then

$X^\alpha X^\beta = X^{\alpha+\beta} \in a$, and so A satisfies the condition (*). Conversely,

$$\left(\sum_{\alpha \in A} c_\alpha X^\alpha\right) \left(\sum_{\beta \in \square^n} d_\beta X^\beta\right) = \sum_{\alpha, \beta} c_\alpha d_\beta X^{\alpha+\beta} \quad (\text{finite sums}),$$

and so if A satisfies (*), then the subspace generated by the monomials $X^\alpha, \alpha \in a$, is an ideal. The proposition gives a classification of the monomial ideals in $k[X_1, \dots, X_n]$: they are in one to one correspondence with the subsets A of \square^n satisfying (*). For example, the monomial ideals in $k[X]$ are exactly the ideals $(X^n), n \geq 1$, and the zero ideal (corresponding to the empty set A). We write $\langle X^\alpha \mid \alpha \in A \rangle$ for the ideal corresponding to A (subspace generated by the $X^\alpha, \alpha \in a$).

LEMMA 1.1. Let S be a subset of \square^n . The ideal a generated by $X^\alpha, \alpha \in S$ is the monomial ideal corresponding to

$$A \stackrel{\text{df}}{=} \left\{ \beta \in \square^n \mid \beta - \alpha \in \square^n, \text{ some } \alpha \in S \right\}$$

Thus, a monomial is in a if and only if it is divisible by one of the $X^\alpha, \alpha \in S$

PROOF. Clearly A satisfies (*), and $a \subset \langle X^\beta \mid \beta \in A \rangle$. Conversely, if $\beta \in A$, then $\beta - \alpha \in \square^n$ for some $\alpha \in S$, and $X^\beta = X^\alpha X^{\beta-\alpha} \in a$. The last statement follows from the fact that $X^\alpha \mid X^\beta \Leftrightarrow \beta - \alpha \in \square^n$. Let $A \subset \square^n$ satisfy (*). From the geometry of A , it is clear that there is a finite set of elements $S = \{\alpha_1, \dots, \alpha_s\}$ of A such that $A = \left\{ \beta \in \square^n \mid \beta - \alpha_i \in \square^2, \text{ some } \alpha_i \in S \right\}$

(The α_i 's are the corners of A) Moreover,

$a \stackrel{\text{df}}{=} \langle X^\alpha \mid \alpha \in A \rangle$ is generated by the monomials $X^{\alpha_i}, \alpha_i \in S$.

DEFINITION 1.0. For a nonzero ideal a in $k[X_1, \dots, X_n]$, we let $(LT(a))$ be the ideal generated by $\{LT(f) \mid f \in a\}$

LEMMA 1.2 Let a be a nonzero ideal in $k[X_1, \dots, X_n]$; then $(LT(a))$ is a monomial ideal, and it equals $(LT(g_1), \dots, LT(g_n))$ for some $g_1, \dots, g_n \in a$.

PROOF. Since $(LT(a))$ can also be described as the ideal generated by the leading monomials (rather than the leading terms) of elements of a .

THEOREM 1.2. Every ideal a in $k[X_1, \dots, X_n]$ is finitely generated; more precisely, $a = (g_1, \dots, g_s)$ where g_1, \dots, g_s are any elements of a whose leading terms generate $LT(a)$

PROOF. Let $f \in a$. On applying the division algorithm, we find $f = a_1 g_1 + \dots + a_s g_s + r$, $a_i, r \in k[X_1, \dots, X_n]$, where either $r = 0$ or no monomial occurring in it is divisible by any $LT(g_i)$. But $r = f - \sum a_i g_i \in a$, and therefore $LT(r) \in LT(a) = (LT(g_1), \dots, LT(g_s))$, implies that every monomial occurring in r is divisible by one in $LT(g_i)$. Thus $r = 0$, and $g \in (g_1, \dots, g_s)$.

DEFINITION 1.1. A finite subset $S = \{g_1, \dots, g_s\}$ of an ideal a is a standard (*Gröbner*) bases for a if $(LT(g_1), \dots, LT(g_s)) = LT(a)$. In other words, S is a standard basis if the leading term of every element of a is divisible by at least one of the leading terms of the g_i .

THEOREM 1.3 The ring $k[X_1, \dots, X_n]$ is Noetherian i.e., every ideal is finitely generated.

PROOF. For $n = 1$, $k[X]$ is a principal ideal domain, which means that every ideal is generated by single element. We shall prove the theorem by induction on n . Note that the obvious map $k[X_1, \dots, X_{n-1}][X_n] \rightarrow k[X_1, \dots, X_n]$ is an isomorphism – this simply says that every polynomial f in n variables X_1, \dots, X_n can be expressed uniquely as a polynomial in X_n with coefficients in $k[X_1, \dots, X_{n-1}]$:

$$f(X_1, \dots, X_n) = a_0(X_1, \dots, X_{n-1})X_n^r + \dots + a_r(X_1, \dots, X_{n-1})$$

Thus the next lemma will complete the proof

LEMMA 1.3. If A is Noetherian, then so also is $A[X]$

PROOF. For a polynomial

$$f(X) = a_0X^r + a_1X^{r-1} + \dots + a_r, \quad a_i \in A, \quad a_0 \neq 0,$$

r is called the degree of f , and a_0 is its leading coefficient. We call 0 the leading coefficient of the polynomial 0 . Let a be an ideal in $A[X]$. The leading coefficients of the polynomials in a form an ideal a' in A , and since A is Noetherian, a' will be finitely generated. Let g_1, \dots, g_m be elements of a whose leading coefficients generate a' , and let r be the maximum degree of g_i . Now let $f \in a$, and suppose f has degree $s > r$, say, $f = aX^s + \dots$. Then $a \in a'$, and so we can write

$$a = \sum b_i a_i, \quad b_i \in A,$$

$a_i = \text{leading coefficient of } g_i$

Now

$$f - \sum b_i g_i X^{s-r_i}, \quad r_i = \text{deg}(g_i), \text{ has degree}$$

$< \text{deg}(f)$. By continuing in this way, we find that $f \equiv f_t \pmod{(g_1, \dots, g_m)}$ With f_t a polynomial of degree $t < r$. For each $d < r$, let a_d be the subset of A consisting of 0 and the leading coefficients of all polynomials in a of degree d ; it is again an ideal in A . Let $g_{d,1}, \dots, g_{d,m_d}$ be polynomials of degree d whose leading coefficients generate a_d . Then the same argument as above shows that any polynomial f_d in a of degree d can be written $f_d \equiv f_{d-1} \pmod{(g_{d,1}, \dots, g_{d,m_d})}$ With f_{d-1} of degree $\leq d-1$. On applying this remark

repeatedly we find that $f_t \in (g_{r-1,1}, \dots, g_{r-1,m_{r-1}}, \dots, g_{0,1}, \dots, g_{0,m_0})$ Hence

$$f_t \in (g_1, \dots, g_m, g_{r-1,1}, \dots, g_{r-1,m_{r-1}}, \dots, g_{0,1}, \dots, g_{0,m_0})$$

and so the polynomials g_1, \dots, g_{0,m_0} generate a

One of the great successes of category theory in computer science has been the development of a “unified theory” of the constructions underlying denotational semantics. In the untyped λ -calculus, any term may appear in the function position of an application. This means that a model D of the λ -calculus must have the property that given a term t whose interpretation is $d \in D$, Also, the interpretation of a functional abstraction like $\lambda x . x$ is most conveniently defined as a function from D to D , which must then be regarded as an element of D . Let $\psi : [D \rightarrow D] \rightarrow D$ be the function that picks out elements of D to represent elements of $[D \rightarrow D]$ and $\phi : D \rightarrow [D \rightarrow D]$ be the function that maps elements of D to functions of D . Since $\psi(f)$ is intended to represent the function f as an element of D , it makes sense to require that $\phi(\psi(f)) = f$, that is, $\psi \circ \psi = id_{[D \rightarrow D]}$ Furthermore, we often want to view every element of D as representing some function from D to D and require that elements representing the same function be equal – that is

$$\psi(\phi(d)) = d$$

or

$$\psi \circ \phi = id_D$$

The latter condition is called extensionality. These conditions together imply that ϕ and ψ are inverses--- that is, D is isomorphic to the space of functions from D to D that can be the interpretations of functional abstractions:

$$D \cong [D \rightarrow D]$$

.Let us suppose we are working with the untyped λ -calculus, we need a solution of the equation $D \cong A + [D \rightarrow D]$, where A is some predetermined domain containing interpretations for elements of C . Each element of D corresponds to either an element of A or an element of $[D \rightarrow D]$, with a tag. This equation can be solved by finding least fixed points of the function $F(X) = A + [X \rightarrow X]$ from domains to domains --- that is, finding domains X such that

$X \cong A + [X \rightarrow X]$, and such that for any domain Y also satisfying this equation, there is an embedding of X to Y --- a pair of maps

$$X \begin{array}{c} \xrightarrow{f} \\ \square \\ \xleftarrow{f^R} \end{array} Y$$

Such that

$$f^R \circ f = id_X$$

$$f \circ f^R \subseteq id_Y$$

Where $f \subseteq g$ means that

f approximates g in some ordering representing their information content. The key shift of perspective from the domain-theoretic to the more general category-theoretic approach lies in considering F not as a function on domains, but as a functor on a category of domains. Instead of a least fixed point of the function, F .

Definition 1.3: Let K be a category and $F: K \rightarrow K$ as a functor. A fixed point of F is a pair (A, a) , where A is a K -object and $a: F(A) \rightarrow A$ is an isomorphism. A prefixed point of F is a pair (A, a) , where A is a K -object and a is any arrow from $F(A)$ to A .

Definition 1.4: An ω -chain in a category K is a diagram of the following form:

$$\Delta = D_0 \xrightarrow{f_0} D_1 \xrightarrow{f_1} D_2 \xrightarrow{f_2} \dots$$

Recall that a cocone μ of an ω -chain Δ is a K -object X and a collection of K -arrows $\{\mu_i: D_i \rightarrow X \mid i \geq 0\}$ such that $\mu_i = \mu_{i+1} \circ f_i$ for all $i \geq 0$. We sometimes write $\mu: \Delta \rightarrow X$ as a reminder of the arrangement of μ 's components. Similarly, a colimit $\mu: \Delta \rightarrow X$ is a cocone with the property that if $\nu: \Delta \rightarrow X'$ is also a cocone then there exists a unique mediating arrow $k: X \rightarrow X'$ such that for all $i \geq 0$, $\nu_i = k \circ \mu_i$. Colimits of ω -chains are sometimes referred to as ω -colimits. Dually, an ω^{op} -chain in K is a diagram of the following form:

$$\Delta = D_0 \xleftarrow{f_0} D_1 \xleftarrow{f_1} D_2 \xleftarrow{f_2} \dots$$

A cone $\mu: X \rightarrow \Delta$ of an ω^{op} -chain Δ is a K -object X and a collection of K -arrows $\{\mu_i: D_i \mid i \geq 0\}$ such that for all $i \geq 0$, $\mu_i = f_i \circ \mu_{i+1}$. An ω^{op} -limit of an ω^{op} -chain Δ is a cone $\mu: X \rightarrow \Delta$ with the property that if $\nu: X' \rightarrow \Delta$ is also a cone, then there exists a unique mediating arrow

$k: X' \rightarrow X$ such that for all $i \geq 0$, $\mu_i \circ k = \nu_i$.

We write \perp_k (or just \perp) for the distinguish initial object of K , when it has one, and $\perp \rightarrow A$ for the unique arrow from \perp to each K -object A . It is also

convenient to write $\Delta^- = D_1 \xrightarrow{f_1} D_2 \xrightarrow{f_2} \dots$ to denote all of Δ except D_0 and f_0 . By analogy,

μ^- is $\{\mu_i \mid i \geq 1\}$. For the images of Δ and μ under

$$F \begin{array}{c} \xrightarrow{F(f_0)} \\ \xrightarrow{F(f_1)} \\ \xrightarrow{F(f_2)} \end{array} \text{ we write } F(\Delta) = F(D_0) \rightarrow F(D_1) \rightarrow F(D_2) \rightarrow \dots$$

$$\text{and } F(\mu) = \{F(\mu_i) \mid i \geq 0\}$$

We write F^i for the i -fold iterated composition of F that is, $F^0(f) = f, F^1(f) = F(f), F^2(f) = F(F(f))$, etc. With these definitions we can state that every monotonic function on a complete lattice has a least fixed point:

Lemma 1.4. Let K be a category with initial object \perp and let $F: K \rightarrow K$ be a functor. Define the ω -chain Δ by

$$\Delta = \perp \xrightarrow{\perp \rightarrow F(\perp)} F(\perp) \xrightarrow{F(\perp \rightarrow F(\perp))} F^2(\perp) \xrightarrow{F^2(\perp \rightarrow F(\perp))} \dots$$

If both $\mu: \Delta \rightarrow D$ and $F(\mu): F(\Delta) \rightarrow F(D)$ are colimits, then (D, d) is an initial F -algebra, where $d: F(D) \rightarrow D$ is the mediating arrow from $F(\mu)$ to the cocone μ^- .

Theorem 1.4 Let a DAG G given in which each node is a random variable, and let a discrete conditional probability distribution of each node given values of its parents in G be specified. Then the product of these conditional distributions yields a joint probability distribution P of the variables, and (G, P) satisfies the Markov condition.

Proof. Order the nodes according to an ancestral ordering. Let X_1, X_2, \dots, X_n be the resultant ordering. Next define.

$$P(x_1, x_2, \dots, x_n) = P(x_n \mid pa_n) P(x_{n-1} \mid pa_{n-1}) \dots P(x_2 \mid pa_2) P(x_1 \mid pa_1),$$

Where PA_i is the set of parents of X_i in G and $P(x_i \mid pa_i)$ is the specified conditional probability distribution. First we show this does indeed yield a joint probability distribution. Clearly, $0 \leq P(x_1, x_2, \dots, x_n) \leq 1$ for all values of the variables. Therefore, to show we have a joint

distribution, as the variables range through all their possible values, is equal to one. To that end, Specified conditional distributions are the conditional distributions they notationally represent in the joint distribution. Finally, we show the Markov condition is satisfied. To do this, we need show for $1 \leq k \leq n$ that

whenever

$$P(pa_k) \neq 0, \text{ if } P(nd_k | pa_k) \neq 0$$

$$\text{and } P(x_k | pa_k) \neq 0$$

$$\text{then } P(x_k | nd_k, pa_k) = P(x_k | pa_k),$$

Where ND_k is the set of nondescendents of X_k of in G . Since $PA_k \subseteq ND_k$, we need only show

$P(x_k | nd_k) = P(x_k | pa_k)$. First for a given k , order the nodes so that all and only nondescendents of X_k precede X_k in the ordering. Note that this ordering depends on k , whereas the ordering in the first part of the proof does not. Clearly then

$$ND_k = \{X_1, X_2, \dots, X_{k-1}\}$$

Let

$$D_k = \{X_{k+1}, X_{k+2}, \dots, X_n\}$$

follows \sum_{d_k}

We define the m^{th} cyclotomic field to be the field $Q[x]/(\Phi_m(x))$ Where $\Phi_m(x)$ is the m^{th} cyclotomic polynomial. $Q[x]/(\Phi_m(x))$ $\Phi_m(x)$ has degree $\varphi(m)$ over Q since $\Phi_m(x)$ has degree $\varphi(m)$. The roots of $\Phi_m(x)$ are just the primitive m^{th} roots of unity, so the complex embeddings of $Q[x]/(\Phi_m(x))$ are simply the $\varphi(m)$ maps

$$\sigma_k : Q[x]/(\Phi_m(x)) \mapsto C,$$

$$1 \leq k < m, (k, m) = 1, \text{ where}$$

$$\sigma_k(x) = \xi_m^k,$$

ξ_m being our fixed choice of primitive m^{th} root of unity. Note that $\xi_m^k \in Q(\xi_m)$ for every k ; it follows that $Q(\xi_m) = Q(\xi_m^k)$ for all k relatively prime to m . In particular, the images of the σ_i coincide, so $Q[x]/(\Phi_m(x))$ is Galois over Q .

This means that we can write $Q(\xi_m)$ for $Q[x]/(\Phi_m(x))$ without much fear of ambiguity;

we will do so from now on, the identification being $\xi_m \mapsto x$. One advantage of this is that one can easily talk about cyclotomic fields being extensions of one another, or intersections or compositums; all of these things take place considering them as subfield of C . We now investigate some basic properties of cyclotomic fields. The first issue is whether or not they are all distinct; to determine this, we need to know which roots of unity lie in $Q(\xi_m)$. Note, for example, that if m is odd, then $-\xi_m$ is a $2m^{\text{th}}$ root of unity. We will show that this is the only way in which one can obtain any non- m^{th} roots of unity.

LEMMA 1.5 If m divides n , then $Q(\xi_m)$ is contained in $Q(\xi_n)$

PROOF. Since $\xi_m^{n/m} = \xi_n$, we have $\xi_m \in Q(\xi_n)$, so the result is clear

LEMMA 1.6 If m and n are relatively prime, then $Q(\xi_m, \xi_n) = Q(\xi_{mn})$

and

$$Q(\xi_m) \cap Q(\xi_n) = Q$$

(Recall the $Q(\xi_m, \xi_n)$ is the compositum of $Q(\xi_m)$ and $Q(\xi_n)$)

PROOF. One checks easily that $\xi_m \xi_n$ is a primitive mn^{th} root of unity, so that

$$Q(\xi_{mn}) \subseteq Q(\xi_m, \xi_n)$$

$$[Q(\xi_m, \xi_n) : Q] \leq [Q(\xi_m) : Q][Q(\xi_n) : Q] = \varphi(m)\varphi(n) = \varphi(mn);$$

Since $[Q(\xi_{mn}) : Q] = \varphi(mn)$; this implies that

$Q(\xi_m, \xi_n) = Q(\xi_{mn})$ We know that $Q(\xi_m, \xi_n)$ has degree $\varphi(mn)$ over Q , so we must have

$$[Q(\xi_m, \xi_n) : Q(\xi_m)] = \varphi(n)$$

and

$$[Q(\xi_m, \xi_n) : Q(\xi_n)] = \varphi(m)$$

$$[Q(\xi_m) : Q(\xi_m) \cap Q(\xi_n)] \geq \varphi(m)$$

And thus that $Q(\xi_m) \cap Q(\xi_n) = Q$

PROPOSITION 1.2 For any m and n

$$Q(\xi_m, \xi_n) = Q(\xi_{[m,n]})$$

And

$$Q(\xi_m) \cap Q(\xi_n) = Q(\xi_{(m,n)});$$

here $[m, n]$ and (m, n) denote the least common multiple and the greatest common divisor of m and n , respectively.

PROOF.

Write

$m = p_1^{e_1} \dots p_k^{e_k}$ and $p_1^{f_1} \dots p_k^{f_k}$ where the p_i are distinct primes. (We allow e_i or f_i to be zero)

$$Q(\xi_m) = Q(\xi_{p_1^{e_1}}) Q(\xi_{p_2^{e_2}}) \dots Q(\xi_{p_k^{e_k}})$$

and

$$Q(\xi_n) = Q(\xi_{p_1^{f_1}}) Q(\xi_{p_2^{f_2}}) \dots Q(\xi_{p_k^{f_k}})$$

Thus

$$\begin{aligned} Q(\xi_m, \xi_n) &= Q(\xi_{p_1^{e_1}}) \dots Q(\xi_{p_2^{e_2}}) Q(\xi_{p_1^{f_1}}) \dots Q(\xi_{p_k^{f_k}}) \\ &= Q(\xi_{p_1^{e_1}}) Q(\xi_{p_1^{f_1}}) \dots Q(\xi_{p_k^{e_k}}) Q(\xi_{p_k^{f_k}}) \\ &= Q(\xi_{p_1^{\max(e_1, f_1)}}) \dots Q(\xi_{p_k^{\max(e_k, f_k)}}) \\ &= Q(\xi_{p_1^{\max(e_1, f_1)} \dots p_k^{\max(e_k, f_k)}}) \\ &= Q(\xi_{[m,n]}); \end{aligned}$$

An entirely similar computation shows that $Q(\xi_m) \cap Q(\xi_n) = Q(\xi_{(m,n)})$

Mutual information measures the information transferred when x_i is sent and y_i is received, and is defined as

$$I(x_i, y_i) = \log_2 \frac{P(x_i/y_i)}{P(x_i)} \text{ bits} \quad (1)$$

In a noise-free channel, each y_i is uniquely connected to the corresponding x_i , and so they constitute an input-output pair (x_i, y_i) for which

$$P(x_i/y_i) = 1 \text{ and } I(x_i, y_i) = \log_2 \frac{1}{P(x_i)} \text{ bits;}$$

that is, the transferred information is equal to the self-information that corresponds to the input x_i . In a very noisy channel, the output y_i and input x_i would be completely uncorrelated, and so $P(x_i/y_i) = P(x_i)$ and also $I(x_i, y_i) = 0$; that is,

there is no transference of information. In general, a given channel will operate between these two extremes. The mutual information is defined

between the input and the output of a given channel. An average of the calculation of the mutual information for all input-output pairs of a given channel is the average mutual information:

$$I(X, Y) = \sum_{i,j} P(x_i, y_j) I(x_i, y_j) = \sum_{i,j} P(x_i, y_j) \log_2 \left[\frac{P(x_i/y_j)}{P(x_i)} \right]$$

bits per symbol. This calculation is done over the input and output alphabets. The average mutual information. The following expressions are useful for modifying the mutual information expression:

$$P(x_i, y_j) = P(x_i/y_j) P(y_j) = P(y_j/x_i) P(x_i)$$

$$P(y_j) = \sum_i P(y_j/x_i) P(x_i)$$

$$P(x_i) = \sum_j P(x_i/y_j) P(y_j)$$

Then

$$\begin{aligned} I(X, Y) &= \sum_{i,j} P(x_i, y_j) \\ &= \sum_{i,j} P(x_i, y_j) \log_2 \left[\frac{1}{P(x_i)} \right] \\ &\quad - \sum_{i,j} P(x_i, y_j) \log_2 \left[\frac{1}{P(x_i/y_j)} \right] \end{aligned}$$

$$\begin{aligned} &= \sum_{i,j} P(x_i, y_j) \log_2 \left[\frac{1}{P(x_i)} \right] \\ &= \sum_i \left[P(x_i/y_j) P(y_j) \right] \log_2 \frac{1}{P(x_i)} \end{aligned}$$

$$\begin{aligned} &= \sum_i P(x_i) \log_2 \frac{1}{P(x_i)} = H(X) \\ &= \sum_i P(x_i) \log_2 \frac{1}{P(x_i)} = H(X) \end{aligned}$$

$$I(X, Y) = H(X) - H(X/Y)$$

$$I(X, Y) = H(X) - H(X/Y)$$

Where

$$H(X/Y) = \sum_{i,j} P(x_i, y_j) \log_2 \frac{1}{P(x_i/y_j)} \text{ is}$$

usually called the equivocation. In a sense, the equivocation can be seen as the information lost in the noisy channel, and is a function of the backward conditional probability. The observation of an output symbol y_j provides $H(X) - H(X/Y)$ bits of information. This difference is the mutual information of the channel. *Mutual Information: Properties* Since

$$P(x_i/y_j)P(y_j) = P(y_j/x_i)P(x_i)$$

The mutual information fits the condition
 $I(X, Y) = I(Y, X)$

And by interchanging input and output it is also true that

$$I(X, Y) = H(Y) - H(Y/X)$$

Where

$$H(Y) = \sum_j P(y_j) \log_2 \frac{1}{P(y_j)}$$

This last entropy is usually called the noise entropy. Thus, the information transferred through the channel is the difference between the output entropy and the noise entropy. Alternatively, it can be said that the channel mutual information is the difference between the number of bits needed for determining a given input symbol before knowing the corresponding output symbol, and the number of bits needed for determining a given input symbol after knowing the corresponding output symbol

$$I(X, Y) = H(X) - H(X/Y)$$

As the channel mutual information expression is a difference between two quantities, it seems that this parameter can adopt negative values. However, and in spite of the fact that for some y_j , $H(X/Y_j)$ can be larger than $H(X)$, this is not possible for the average value calculated over all the outputs:

$$\sum_{i,j} P(x_i, y_j) \log_2 \frac{P(x_i/y_j)}{P(x_i)} = \sum_{i,j} P(x_i, y_j) \log_2 \frac{P(x_i, y_j)}{P(x_i)P(y_j)}$$

Then

$$-I(X, Y) = \sum_{i,j} P(x_i, y_j) \frac{P(x_i)P(y_j)}{P(x_i, y_j)} \leq 0$$

Because this expression is of the form

$$\sum_{i=1}^M P_i \log_2 \left(\frac{Q_i}{P_i} \right) \leq 0$$

The above expression can be applied due to the factor $P(x_i)P(y_j)$, which is the product of two probabilities, so that it behaves as the quantity Q_i , which in this expression is a dummy variable that fits the condition $\sum_i Q_i \leq 1$. It can be concluded that the average mutual information is a non-negative number. It can also be equal to zero, when the input and the output are independent of each other. A related entropy called the joint entropy is defined as

$$\begin{aligned} H(X, Y) &= \sum_{i,j} P(x_i, y_j) \log_2 \frac{1}{P(x_i, y_j)} \\ &= \sum_{i,j} P(x_i, y_j) \log_2 \frac{P(x_i)P(y_j)}{P(x_i, y_j)} \\ &+ \sum_{i,j} P(x_i, y_j) \log_2 \frac{1}{P(x_i)P(y_j)} \end{aligned}$$

Theorem 1.5: Entropies of the binary erasure channel (BEC) The BEC is defined with an alphabet of two inputs and three outputs, with symbol probabilities.

$P(x_1) = \alpha$ and $P(x_2) = 1 - \alpha$, and transition probabilities

$$P(y_3/x_2) = 1 - p \text{ and } P(y_2/x_1) = 0,$$

$$\text{and } P(y_3/x_1) = 0$$

$$\text{and } P(y_1/x_2) = p$$

$$\text{and } P(y_2/x_2) = 1 - p$$

Lemma 1.7. Given an arbitrary restricted time-discrete, amplitude-continuous channel whose restrictions are determined by sets F_n and whose density functions exhibit no dependence on the state s , let n be a fixed positive integer, and $p(x)$ an arbitrary probability density function on Euclidean n -space. $p(y|x)$ for the density $p_n(y_1, \dots, y_n | x_1, \dots, x_n)$ and F for F_n . For any real number a , let

$$A = \left\{ (x, y) : \log \frac{p(y|x)}{p(y)} > a \right\} \quad (1)$$

Then for each positive integer u , there is a code (u, n, λ) such that

$$\lambda \leq ue^{-a} + P\{(X, Y) \notin A\} + P\{X \notin F\} \quad (2)$$

Where

$$P\{(X, Y) \in A\} = \int_A \dots \int p(x, y) dx dy, \quad p(x, y) = p(x)p(y|x)$$

and

$$P\{X \in F\} = \int_F \dots \int p(x) dx$$

Proof: A sequence $x^{(1)} \in F$ such that

$$P\{Y \in A_{x^{(1)}} | X = x^{(1)}\} \geq 1 - \epsilon$$

where $A_x = \{y : (x, y) \in A\}$;

Choose the decoding set B_1 to be $A_{x^{(1)}}$. Having chosen $x^{(1)}, \dots, x^{(k-1)}$ and B_1, \dots, B_{k-1} , select $x^k \in F$ such that

$$P\left\{Y \in A_{x^{(k)}} - \bigcup_{i=1}^{k-1} B_i \mid X = x^{(k)}\right\} \geq 1 - \varepsilon;$$

Set $B_k = A_{x^{(k)}} - \bigcup_{i=1}^{k-1} B_i$, If the process does not terminate in a finite number of steps, then the sequences $x^{(i)}$ and decoding sets $B_i, i = 1, 2, \dots, u$, form the desired code. Thus assume that the process terminates after t steps. (Conceivably $t = 0$). We will show $t \geq u$ by showing that $\varepsilon \leq te^{-a} + P\{(X, Y) \notin A\} + P\{X \notin F\}$. We proceed as follows.

Let

$$B = \bigcup_{j=1}^t B_j. \text{ (If } t = 0, \text{ take } B = \phi). \text{ Then}$$

$$P\{(X, Y) \in A\} = \int_{(x,y) \in A} p(x, y) dx dy$$

$$= \int_x p(x) \int_{y \in A_x} p(y | x) dy dx$$

$$= \int_x p(x) \int_{y \in B \cap A_x} p(y | x) dy dx + \int_x p(x)$$

Algorithms

Ideals. Let A be a ring. Recall that an ideal a in A is a subset such that a is subgroup of A regarded as a group under addition;

$$a \in a, r \in A \Rightarrow ra \in a$$

The ideal generated by a subset S of A is the intersection of all ideals A containing a ----- it is easy to verify that this is in fact an ideal, and that it consist of all finite sums of the form $\sum r_i s_i$ with $r_i \in A, s_i \in S$. When $S = \{s_1, \dots, s_m\}$, we shall write (s_1, \dots, s_m) for the ideal it generates.

Let a and b be ideals in A. The set $\{a+b \mid a \in a, b \in b\}$ is an ideal, denoted by $a+b$. The ideal generated by $\{ab \mid a \in a, b \in b\}$ is denoted by ab . Note that $ab \subset a \cap b$. Clearly ab consists of all finite sums $\sum a_i b_i$ with $a_i \in a$ and $b_i \in b$, and if $a = (a_1, \dots, a_m)$ and $b = (b_1, \dots, b_n)$, then $ab = (a_1 b_1, \dots, a_i b_j, \dots, a_m b_n)$. Let a be an ideal of A. The set of cosets of a in A forms a ring A/a , and $a \mapsto a+a$ is a homomorphism $\phi: A \mapsto A/a$. The map $b \mapsto \phi^{-1}(b)$ is a one to one correspondence between the ideals of A/a and the ideals of A containing a. An ideal p is prime if $p \neq A$ and $ab \in p \Rightarrow a \in p$ or $b \in p$.

Thus p is prime if and only if A/p is nonzero and has the property that $ab = 0, b \neq 0 \Rightarrow a = 0$, i.e., A/p is an integral domain. An ideal m is maximal if $m \neq A$ and there does not exist an ideal n contained strictly between m and A. Thus m is maximal if and only if A/m has no proper nonzero ideals, and so is a field. Note that m maximal \Rightarrow m prime. The ideals of $A \times B$ are all of the form $a \times b$, with a and b ideals in A and B. To see this, note that if c is an ideal in $A \times B$ and $(a, b) \in c$, then $(a, 0) = (a, b)(1, 0) \in c$ and $(0, b) = (a, b)(0, 1) \in c$. This shows that $c = a \times b$ with $a = \{a \mid (a, b) \in c \text{ some } b \in b\}$ and $b = \{b \mid (a, b) \in c \text{ some } a \in a\}$

Let A be a ring. An A-algebra is a ring B together with a homomorphism $i_B: A \rightarrow B$. A homomorphism of A-algebra $B \rightarrow C$ is a homomorphism of rings $\phi: B \rightarrow C$ such that $\phi(i_B(a)) = i_C(a)$ for all $a \in A$. An A-algebra B is said to be finitely generated (or of finite-type over A) if there exist elements $x_1, \dots, x_n \in B$ such that every element of B can be expressed as a polynomial in the x_i with coefficients in $i(A)$, i.e., such that the homomorphism $A[X_1, \dots, X_n] \rightarrow B$ sending X_i to x_i is surjective. A ring homomorphism $A \rightarrow B$ is finite, and B is finitely generated as an A-module. Let k be a field, and let A be a k-algebra. If $1 \neq 0$ in A, then the map $k \rightarrow A$ is injective, we can identify k with its image, i.e., we can regard k as a subring of A. If $1=0$ in a ring R, the R is the zero ring, i.e., $R = \{0\}$.

Polynomial rings. Let k be a field. A monomial in X_1, \dots, X_n is an expression of the form $X_1^{a_1} \dots X_n^{a_n}$, $a_j \in N$. The total degree of the monomial is $\sum a_i$. We sometimes abbreviate it by $X^\alpha, \alpha = (a_1, \dots, a_n) \in \mathbb{N}^n$. The elements of the polynomial ring $k[X_1, \dots, X_n]$ are finite sums $\sum c_{a_1, \dots, a_n} X_1^{a_1} \dots X_n^{a_n}$, $c_{a_1, \dots, a_n} \in k, a_j \in \mathbb{N}$. With the obvious notions of equality, addition and multiplication. Thus the monomials form basis for

$k[X_1, \dots, X_n]$ as a k -vector space. The ring $k[X_1, \dots, X_n]$ is an integral domain, and the only units in it are the nonzero constant polynomials. A polynomial $f(X_1, \dots, X_n)$ is *irreducible* if it is nonconstant and has only the obvious factorizations, i.e., $f = gh \Rightarrow g$ or h is constant. **Division in $k[X]$.** The division algorithm allows us to divide a nonzero polynomial into another: let f and g be polynomials in $k[X]$ with $g \neq 0$; then there exist unique polynomials $q, r \in k[X]$ such that $f = qg + r$ with either $r = 0$ or $\deg r < \deg g$. Moreover, there is an algorithm for deciding whether $f \in (g)$, namely, find r and check whether it is zero. Moreover, the Euclidean algorithm allows to pass from finite set of generators for an ideal in $k[X]$ to a single generator by successively replacing each pair of generators with their greatest common divisor. (Pure) **lexicographic ordering (lex).** Here monomials are ordered by lexicographic (dictionary) order. More precisely, let $\alpha = (a_1, \dots, a_n)$ and $\beta = (b_1, \dots, b_n)$ be two elements of \mathbb{N}^n ; then $\alpha > \beta$ and $X^\alpha > X^\beta$ (lexicographic ordering) if, in the vector difference $\alpha - \beta \in \mathbb{N}^n$, the left most nonzero entry is positive. For example,

$XY^2 > Y^3Z^4$; $X^3Y^2Z^4 > X^3Y^2Z$. Note that this isn't quite how the dictionary would order them: it would put $XXXYYYZZZ$ after $XXXYYZ$. **Graded reverse lexicographic order (grevlex).** Here monomials are ordered by total degree, with ties broken by reverse lexicographic ordering. Thus, $\alpha > \beta$ if $\sum a_i > \sum b_i$, or $\sum a_i = \sum b_i$ and in $\alpha - \beta$ the right most nonzero entry is negative. For example:

$$X^4Y^4Z^7 > X^5Y^5Z^4 \quad (\text{total degree greater})$$

$$XY^5Z^2 > X^4YZ^3, \quad X^5YZ > X^4YZ^2$$

Orderings on $k[X_1, \dots, X_n]$. Fix an ordering on the monomials in $k[X_1, \dots, X_n]$. Then we can write an element f of $k[X_1, \dots, X_n]$ in a canonical fashion, by re-ordering its elements in decreasing order. For example, we would write

$$f = 4XY^2Z + 4Z^2 - 5X^3 + 7X^2Z^2$$

as

$$f = -5X^3 + 7X^2Z^2 + 4XY^2Z + 4Z^2 \quad (\text{lex})$$

or

$$f = 4XY^2Z + 7X^2Z^2 - 5X^3 + 4Z^2 \quad (\text{grevlex})$$

Let $\sum a_\alpha X^\alpha \in k[X_1, \dots, X_n]$, in decreasing order:

$$f = a_{\alpha_0} X^{\alpha_0} + a_{\alpha_1} X^{\alpha_1} + \dots, \quad \alpha_0 > \alpha_1 > \dots, \quad \alpha_0 \neq 0$$

Then we define.

- The *multidegree* of f to be $\text{multdeg}(f) = \alpha_0$;
- The *leading coefficient* of f to be $LC(f) = a_{\alpha_0}$;
- The *leading monomial* of f to be $LM(f) = X^{\alpha_0}$;
- The *leading term* of f to be $LT(f) = a_{\alpha_0} X^{\alpha_0}$

For the polynomial $f = 4XY^2Z + \dots$, the multidegree is (1,2,1), the leading coefficient is 4, the leading monomial is XY^2Z , and the leading term is $4XY^2Z$. **The division algorithm in $k[X_1, \dots, X_n]$.** Fix a monomial ordering in \mathbb{N}^n . Suppose given a polynomial f and an ordered set (g_1, \dots, g_s) of polynomials; the division algorithm then constructs polynomials a_1, \dots, a_s and r such that $f = a_1g_1 + \dots + a_sg_s + r$ Where either $r = 0$ or no monomial in r is divisible by any of $LT(g_1), \dots, LT(g_s)$ **Step 1:** If $LT(g_1) | LT(f)$, divide g_1 into f to get

$$f = a_1g_1 + h, \quad a_1 = \frac{LT(f)}{LT(g_1)} \in k[X_1, \dots, X_n]$$

If $LT(g_1) | LT(h)$, repeat the process until $f = a_1g_1 + f_1$ (different a_1) with $LT(f_1)$ not divisible by $LT(g_1)$. Now divide g_2 into f_1 , and so on, until $f = a_1g_1 + \dots + a_sg_s + r_1$ With $LT(r_1)$ not divisible by any $LT(g_1), \dots, LT(g_s)$

Step 2: Rewrite $r_1 = LT(r_1) + r_2$, and repeat Step 1 with r_2 for f :

$$f = a_1g_1 + \dots + a_sg_s + LT(r_1) + r_3 \quad (\text{different } a_i's)$$

Monomial ideals. In general, an ideal a will contain a polynomial without containing the

individual terms of the polynomial; for example, the ideal $a = (Y^2 - X^3)$ contains $Y^2 - X^3$ but not Y^2 or X^3 .

DEFINITION 1.5. An ideal a is *monomial* if $\sum c_\alpha X^\alpha \in a \Rightarrow X^\alpha \in a$ all α with $c_\alpha \neq 0$.

PROPOSITION 1.3. Let a be a *monomial ideal*, and let $A = \{\alpha \mid X^\alpha \in a\}$. Then A satisfies the condition $\alpha \in A, \beta \in \square^n \Rightarrow \alpha + \beta \in A$ (*). And a is the k -subspace of $k[X_1, \dots, X_n]$ generated by the $X^\alpha, \alpha \in A$. Conversely, if A is a subset of \square^n satisfying (*), then the k -subspace a of $k[X_1, \dots, X_n]$ generated by $\{X^\alpha \mid \alpha \in A\}$ is a monomial ideal.

PROOF. It is clear from its definition that a monomial ideal a is the k -subspace of $k[X_1, \dots, X_n]$ generated by the set of monomials it contains. If $X^\alpha \in a$ and $X^\beta \in k[X_1, \dots, X_n]$.

If a permutation is chosen uniformly and at random from the $n!$ possible permutations in S_n , then the counts $C_j^{(n)}$ of cycles of length j are dependent random variables. The joint distribution of $C^{(n)} = (C_1^{(n)}, \dots, C_n^{(n)})$ follows from Cauchy's formula, and is given by

$$P[C^{(n)} = c] = \frac{1}{n!} N(n, c) = 1 \left\{ \sum_{j=1}^n j c_j = n \right\} \prod_{j=1}^n \left(\frac{1}{j} \right)^{c_j} \frac{1}{c_j!}, \quad (1.1)$$

for $c \in \square_+^n$.

Lemma 1.7 For nonnegative integers m_1, \dots, m_n ,

$$E \left(\prod_{j=1}^n (C_j^{(n)})^{m_j} \right) = \left(\prod_{j=1}^n \left(\frac{1}{j} \right)^{m_j} \right) 1 \left\{ \sum_{j=1}^n j m_j \leq n \right\} \quad (1.4)$$

Proof. This can be established directly by exploiting cancellation of the form $c_j^{[m_j]} / c_j! = 1 / (c_j - m_j)!$ when $c_j \geq m_j$, which occurs between the ingredients in Cauchy's formula and the falling factorials in the moments. Write $m = \sum j m_j$. Then, with the first sum indexed by $c = (c_1, \dots, c_n) \in \square_+^n$ and the last sum indexed by

$d = (d_1, \dots, d_n) \in \square_+^n$ via the correspondence $d_j = c_j - m_j$, we have

$$\begin{aligned} E \left(\prod_{j=1}^n (C_j^{(n)})^{m_j} \right) &= \sum_c P[C^{(n)} = c] \prod_{j=1}^n (c_j)^{m_j} \\ &= \sum_{c: c_j \geq m_j \text{ for all } j} 1 \left\{ \sum_{j=1}^n j c_j = n \right\} \prod_{j=1}^n \frac{(c_j)^{m_j}}{j^{c_j} c_j!} \\ &= \prod_{j=1}^n \frac{1}{j^{m_j}} \sum_d 1 \left\{ \sum_{j=1}^n j d_j = n - m \right\} \prod_{j=1}^n \frac{1}{j^{d_j} (d_j)!} \end{aligned}$$

This last sum simplifies to the indicator $1(m \leq n)$, corresponding to the fact that if $n - m \geq 0$, then $d_j = 0$ for $j > n - m$, and a random permutation in S_{n-m} must have some cycle structure (d_1, \dots, d_{n-m}) . The moments of $C_j^{(n)}$ follow immediately as

$$E(C_j^{(n)})^{[r]} = j^{-r} 1\{jr \leq n\} \quad (1.2)$$

We note for future reference that (1.4) can also be written in the form

$$E \left(\prod_{j=1}^n (C_j^{(n)})^{m_j} \right) = E \left(\prod_{j=1}^n Z_j^{m_j} \right) 1 \left\{ \sum_{j=1}^n j m_j \leq n \right\}, \quad (1.3)$$

Where the Z_j are independent Poisson-distribution random variables that satisfy $E(Z_j) = 1/j$

The marginal distribution of cycle counts provides a formula for the joint distribution of the cycle counts C_j^n , we find the distribution of C_j^n using a combinatorial approach combined with the inclusion-exclusion formula.

Lemma 1.8. For $1 \leq j \leq n$,

$$P[C_j^{(n)} = k] = \frac{j^{-k}}{k!} \sum_{l=0}^{[n/j]-k} (-1)^l \frac{j^{-l}}{l!} \quad (1.1)$$

Proof. Consider the set I of all possible cycles of length j , formed with elements chosen from $\{1, 2, \dots, n\}$, so that $|I| = n^{[l]j/j}$. For each $\alpha \in I$, consider the "property" G_α of having α ; that is, G_α is the set of permutations $\pi \in S_n$ such that α is one of the cycles of π . We then have $|G_\alpha| = (n - j)!$, since the elements of $\{1, 2, \dots, n\}$ not in α must be permuted among themselves. To use the inclusion-exclusion formula we need to calculate the term S_r , which is the sum of the probabilities of the r -fold intersection of properties, summing over all sets of r distinct properties. There are two cases to consider. If the r properties are

indexed by r cycles having no elements in common, then the intersection specifies how rj elements are moved by the permutation, and there are $(n-rj)!(rj \leq n)$ permutations in the intersection. There are $n^{\lfloor rj \rfloor} / (j^r r!)$ such intersections. For the other case, some two distinct properties name some element in common, so no permutation can have both these properties, and the r -fold intersection is empty. Thus

$$S_r = (n-rj)!(rj \leq n) \\ \times \frac{n^{\lfloor rj \rfloor}}{j^r r! n!} = 1(rj \leq n) \frac{1}{j^r r!}$$

Finally, the inclusion-exclusion series for the number of permutations having exactly k properties is

$$\sum_{l \geq 0} (-1)^l \binom{k+l}{l} S_{k+l}$$

Which simplifies to (1.1) Returning to the original hat-check problem, we substitute $j=1$ in (1.1) to obtain the distribution of the number of fixed points of a random permutation. For $k = 0, 1, \dots, n$,

$$P[C_1^{(n)} = k] = \frac{1}{k!} \sum_{l=0}^{n-k} (-1)^l \frac{1}{l!}, \quad (1.2)$$

and the moments of $C_1^{(n)}$ follow from (1.2) with $j=1$. In particular, for $n \geq 2$, the mean and variance of $C_1^{(n)}$ are both equal to 1. The joint distribution of $(C_1^{(n)}, \dots, C_b^{(n)})$ for any $1 \leq b \leq n$ has an expression similar to (1.7); this too can be derived by inclusion-exclusion. For any $c = (c_1, \dots, c_b) \in \square_+^b$ with $m = \sum c_i$,

$$P[(C_1^{(n)}, \dots, C_b^{(n)}) = c] \\ = \left\{ \prod_{i=1}^b \binom{1}{i}^{c_i} \frac{1}{c_i!} \right\} \sum_{\substack{l \geq 0 \text{ with} \\ \sum l_i \leq n-m}} (-1)^{l_1 + \dots + l_b} \prod_{i=1}^b \binom{1}{i}^{l_i} \frac{1}{l_i!} \quad (1.3)$$

The joint moments of the first b counts $C_1^{(n)}, \dots, C_b^{(n)}$ can be obtained directly from (1.2) and (1.3) by setting $m_{b+1} = \dots = m_n = 0$

The limit distribution of cycle counts

It follows immediately from Lemma 1.2 that for each fixed j , as $n \rightarrow \infty$,

$$P[C_j^{(n)} = k] \rightarrow \frac{j^{-k}}{k!} e^{-1/j}, \quad k = 0, 1, 2, \dots,$$

So that $C_j^{(n)}$ converges in distribution to a random variable Z_j having a Poisson distribution with

mean $1/j$; we use the notation $C_j^{(n)} \rightarrow_d Z_j$ where $Z_j \square P_o(1/j)$ to describe this. Infact, the limit random variables are independent.

Theorem 1.6 The process of cycle counts converges in distribution to a Poisson process of \square with intensity j^{-1} . That is, as $n \rightarrow \infty$,

$$(C_1^{(n)}, C_2^{(n)}, \dots) \rightarrow_d (Z_1, Z_2, \dots) \quad (1.1)$$

Where the $Z_j, j = 1, 2, \dots$, are independent Poisson-distributed random variables with $E(Z_j) = \frac{1}{j}$

Proof. To establish the converges in distribution one shows that for each fixed $b \geq 1$, as $n \rightarrow \infty$,

$$P[(C_1^{(n)}, \dots, C_b^{(n)}) = c] \rightarrow P[(Z_1, \dots, Z_b) = c]$$

Error rates

The proof of Theorem says nothing about the rate of convergence. Elementary analysis can be used to estimate this rate when $b=1$. Using properties of alternating series with decreasing terms, for $k = 0, 1, \dots, n$,

$$\frac{1}{k!} \left(\frac{1}{(n-k+1)!} - \frac{1}{(n-k+2)!} \right) \leq |P[C_1^{(n)} = k] - P[Z_1 = k]| \\ \leq \frac{1}{k!(n-k+1)!}$$

It follows that

$$\frac{2^{n+1}}{(n+1)!} \frac{n}{n+2} \leq \sum_{k=0}^n |P[C_1^{(n)} = k] - P[Z_1 = k]| \leq \frac{2^{n+1}-1}{(n+1)!} \quad (1.11)$$

Since

$$P[Z_1 > n] = \frac{e^{-1}}{(n+1)!} \left(1 + \frac{1}{n+2} + \frac{1}{(n+2)(n+3)} + \dots \right) < \frac{1}{(n+1)!}$$

We see from (1.11) that the total variation distance between the distribution $L(C_1^{(n)})$ of $C_1^{(n)}$ and the distribution $L(Z_1)$ of Z_1

Establish the asymptotics of $P[A_n(C^{(n)})]$ under conditions (A_0) and (B_{01}) , where

$$A_n(C^{(n)}) = \bigcap_{1 \leq i \leq n} \bigcap_{r_i+1 \leq j \leq r_i} \{C_{ij}^{(n)} = 0\},$$

and $\zeta_i = (r_i' / r_{id}) - 1 = O(i^{-g})$ as $i \rightarrow \infty$, for some $g' > 0$. We start with the expression

$$P[A_n(C^{(n)})] = \frac{P[T_{0m}(Z') = n]}{P[T_{0m}(Z) = n]}$$

$$\prod_{\substack{1 \leq i \leq n \\ r_i + 1 \leq j \leq r_i}} \left\{ 1 - \frac{\theta}{ir_i} (1 + E_{i0}) \right\} \quad (1.1)$$

$$P[T_{0n}(Z') = n]$$

$$= \frac{\theta d}{n} \exp \left\{ \sum_{i \geq 1} [\log(1 + i^{-1} \theta d) - i^{-1} \theta d] \right\}$$

$$\left\{ 1 + O(n^{-1} \phi_{\{1,2,7\}}^*(n)) \right\} \quad (1.2)$$

and

$$P[T_{0n}(Z) = n]$$

$$= \frac{\theta d}{n} \exp \left\{ \sum_{i \geq 1} [\log(1 + i^{-1} \theta d) - i^{-1} \theta d] \right\}$$

$$\left\{ 1 + O(n^{-1} \phi_{\{1,2,7\}}^*(n)) \right\} \quad (1.3)$$

Where $\phi_{\{1,2,7\}}^*(n)$ refers to the quantity derived from Z' . It thus follows that $P[A_n(C^{(n)})] \square Kn^{-\theta(1-d)}$ for a constant K , depending on Z and the r_i and computable explicitly from (1.1) – (1.3), if Conditions (A_0) and (B_{01}) are satisfied and if $\zeta_i^* = O(i^{-g'})$ from some $g' > 0$, since, under these circumstances, both $n^{-1} \phi_{\{1,2,7\}}^*(n)$ and $n^{-1} \phi_{\{1,2,7\}}(n)$ tend to zero as $n \rightarrow \infty$. In particular, for polynomials and square free polynomials, the relative error in this asymptotic approximation is of order n^{-1} if $g' > 1$.

For $0 \leq b \leq n/8$ and $n \geq n_0$, with n_0

$$d_{TV}(L(C[1,b]), L(Z[1,b]))$$

$$\leq d_{TV}(L(C[1,b]), L(Z[1,b]))$$

$$\leq \varepsilon_{\{7,7\}}(n,b),$$

Where $\varepsilon_{\{7,7\}}(n,b) = O(b/n)$ under Conditions $(A_0), (D_1)$ and (B_{11}) . Since, by the Conditioning Relation,

$$L(C[1,b] | T_{0b}(C) = l) = L(Z[1,b] | T_{0b}(Z) = l),$$

It follows by direct calculation that

$$d_{TV}(L(C[1,b]), L(Z[1,b]))$$

$$= d_{TV}(L(T_{0b}(C)), L(T_{0b}(Z)))$$

$$= \max_A \sum_{r \in A} P[T_{0b}(Z) = r]$$

$$\left\{ 1 - \frac{P[T_{bn}(Z) = n-r]}{P[T_{0n}(Z) = n]} \right\} \quad (1.4)$$

Suppressing the argument Z from now on, we thus obtain

$$d_{TV}(L(C[1,b]), L(Z[1,b]))$$

$$= \sum_{r \geq 0} P[T_{0b} = r] \left\{ 1 - \frac{P[T_{bn} = n-r]}{P[T_{0n} = n]} \right\}_+$$

$$\leq \sum_{r > n/2} P[T_{0b} = r] + \sum_{r=0}^{[n/2]} \frac{P[T_{0b} = r]}{P[T_{0b} = n]}$$

$$\times \left\{ \sum_{s=0}^n P[T_{0b} = s] (P[T_{bn} = n-s] - P[T_{bn} = n-r]) \right\}_+$$

$$\leq \sum_{r > n/2} P[T_{0b} = r] + \sum_{r=0}^{[n/2]} P[T_{0b} = r]$$

$$\times \sum_{s=0}^{[n/2]} P[T_{0b} = s] \frac{\{P[T_{bn} = n-s] - P[T_{bn} = n-r]\}}{P[T_{0n} = n]}$$

$$+ \sum_{s=0}^{[n/2]} P[T_{0b} = r] \sum_{s=[n/2]+1}^n P[T = s] P[T_{bn} = n-s] / P[T_{0n} = n]$$

The first sum is at most $2n^{-1}ET_{0b}$; the third is bound by

$$\left(\max_{n/2 < s \leq n} P[T_{0b} = s] \right) / P[T_{0n} = n]$$

$$\leq \frac{2\varepsilon_{\{10.5(1)\}}(n/2, b)}{n} \frac{3n}{\theta P_\theta[0,1]}$$

$$\frac{3n}{\theta P_\theta[0,1]} 4n^{-2} \phi_{\{10.8\}}^*(n) \sum_{r=0}^{[n/2]} P[T_{0b} = r] \sum_{s=0}^{[n/2]} P[T_{0b} = s] \frac{1}{2} |r-s|$$

$$\leq \frac{12\phi_{\{10.8\}}^*(n)}{\theta P_\theta[0,1]} \frac{ET_{0b}}{n}$$

Hence we may take

$$\varepsilon_{\{7,7\}}(n,b) = 2n^{-1}ET_{0b}(Z) \left\{ 1 + \frac{6\phi_{\{10.8\}}^*(n)}{\theta P_\theta[0,1]} \right\} P$$

$$+ \frac{6}{\theta P_\theta[0,1]} \varepsilon_{\{10.5(1)\}}(n/2, b) \quad (1.5)$$

Required order under Conditions $(A_0), (D_1)$ and (B_{11}) , if $S(\infty) < \infty$. If not, $\phi_{\{10.8\}}^*(n)$ can be replaced by $\phi_{\{10.11\}}^*(n)$ in the above, which has the required order, without the

restriction on the r_i implied by $S(\infty) < \infty$. Examining the Conditions $(A_0), (D_1)$ and (B_{11}) , it is perhaps surprising to find that (B_{11}) is required instead of just (B_{01}) ; that is, that we should need $\sum_{l \geq 2} l \varepsilon_{il} = O(i^{-a_1})$ to hold for some $a_1 > 1$. A first observation is that a similar problem arises with the rate of decay of ε_{i1} as well. For this reason, n_1

is replaced by n_1 . This makes it possible to replace condition (A_1) by the weaker pair of conditions (A_0) and (D_1) in the eventual assumptions needed for $\varepsilon_{\{7.7\}}(n, b)$ to be of order $O(b/n)$; the decay rate requirement of order $i^{-1-\gamma}$ is shifted from ε_{i1} itself to its first difference. This is needed to obtain the right approximation error for the random mappings example. However, since all the classical applications make far more stringent assumptions about the $\varepsilon_{il}, l \geq 2$, than are made in (B_{11}) . The critical point of the proof is seen where the initial estimate of the difference $P[T_{bn}^{(m)} = s] - P[T_{bn}^{(m)} = s + 1]$. The factor $\varepsilon_{\{10.10\}}(n)$, which should be small, contains a far

tail element from n_1 of the form $\phi_1^\theta(n) + u_1^*(n)$, which is only small if $a_1 > 1$, being otherwise of order $O(n^{1-a_1+\delta})$ for any $\delta > 0$, since $a_2 > 1$ is in any case assumed. For $s \geq n/2$, this gives rise to a contribution of order $O(n^{-1-a_1+\delta})$ in the estimate of the difference $P[T_{bn} = s] - P[T_{bn} = s + 1]$, which, in the remainder of the proof, is translated into a contribution of order $O(n^{-1-a_1+\delta})$ for differences of the form $P[T_{bn} = s] - P[T_{bn} = s + 1]$, finally leading to a contribution of order $bn^{-a_1+\delta}$ for any $\delta > 0$ in $\varepsilon_{\{7.7\}}(n, b)$. Some improvement would seem to be possible, defining the function g by $g(w) = 1_{\{w=s\}} - 1_{\{w=s+t\}}$, differences that are of the form $P[T_{bn} = s] - P[T_{bn} = s + t]$ can be directly estimated, at a cost of only a single contribution of the form $\phi_1^\theta(n) + u_1^*(n)$. Then, iterating the cycle, in which one estimate of a difference in point probabilities is improved to an estimate of smaller order, a bound of the form

$|P[T_{bn} = s] - P[T_{bn} = s + t]| = O(n^{-2}t + n^{-1-a_1+\delta})$ for any $\delta > 0$ could perhaps be attained, leading to a final error estimate in order $O(bn^{-1} + n^{-a_1+\delta})$ for any $\delta > 0$, to replace $\varepsilon_{\{7.7\}}(n, b)$. This would be of the ideal order $O(b/n)$ for large enough b , but would still be coarser for small b .

With b and n as in the previous section, we wish to show that

$$\left| d_{TV}(L(C[1, b]), L(Z[1, b])) - \frac{1}{2}(n+1)^{-1} |1 - \theta| E|T_{0b} - ET_{0b}| \right| \leq \varepsilon_{\{7.8\}}(n, b),$$

Where $\varepsilon_{\{7.8\}}(n, b) = O(n^{-1}b[n^{-1}b + n^{-\beta_{12}+\delta}])$ for any $\delta > 0$ under Conditions $(A_0), (D_1)$ and (B_{12}) , with β_{12} . The proof uses sharper estimates. As before, we begin with the formula

$$d_{TV}(L(C[1, b]), L(Z[1, b])) = \sum_{r \geq 0} P[T_{0b} = r] \left\{ 1 - \frac{P[T_{bn} = n - r]}{P[T_{0n} = n]} \right\}_+$$

Now we observe that

$$\begin{aligned} & \left| \sum_{r \geq 0} P[T_{0b} = r] \left\{ 1 - \frac{P[T_{bn} = n - r]}{P[T_{0n} = n]} \right\}_+ - \sum_{r=0}^{\lfloor n/2 \rfloor} \frac{P[T_{0b} = r]}{P[T_{0n} = n]} \right| \\ & \times \left| \sum_{s=\lfloor n/2 \rfloor + 1}^n P[T_{0b} = s] (P[T_{bn} = n - s] - P[T_{bn} = n - r]) \right| \\ & \leq 4n^{-2} ET_{0b}^2 + (\max_{n/2 < s \leq n} P[T_{0b} = s]) / P[T_{0n} = n] \\ & + P[T_{0b} > n/2] \\ & \leq 8n^{-2} ET_{0b}^2 + \frac{3\varepsilon_{\{10.5(2)\}}(n/2, b)}{\theta P_\theta[0, 1]}, \end{aligned} \tag{1.1}$$

We have

$$\left| \sum_{r=0}^{\lfloor n/2 \rfloor} \frac{P[T_{0b} = r]}{P[T_{0n} = n]} \right|$$

$$\times \left\{ \sum_{s=0}^{\lfloor n/2 \rfloor} P[T_{0b} = s] (P[T_{bn} = n-s] - P[T_{bn} = n-r]) \right\}_+$$

$$- \left\{ \sum_{s=0}^{\lfloor n/2 \rfloor} P[T_{0b} = s] \frac{(s-r)(1-\theta)}{n+1} P[T_{0n} = n] \right\}_+ \quad |$$

$$\leq \frac{1}{n^2 P[T_{0n} = n]} \sum_{r \geq 0} P[T_{0b} = r] \sum_{s \geq 0} P[T_{0b} = s] |s-r|$$

$$\times \left\{ \varepsilon_{\{10.14\}}(n, b) + 2(r \vee s) |1-\theta| n^{-1} \left\{ K_0 \theta + 4\phi_{\{10.8\}}^*(n) \right\} \right\}$$

$$\leq \frac{6}{\theta n P_\theta[0,1]} ET_{0b} \varepsilon_{\{10.14\}}(n, b)$$

$$+ 4|1-\theta| n^{-2} ET_{0b}^2 \left\{ K_0 \theta + 4\phi_{\{10.8\}}^*(n) \right\}$$

$$\left(\frac{3}{\theta n P_\theta[0,1]} \right), \quad (1.2)$$

The approximation in (1.2) is further simplified by noting that

$$\sum_{r=0}^{\lfloor n/2 \rfloor} P[T_{0b} = r] \left| \left\{ \sum_{s=0}^{\lfloor n/2 \rfloor} P[T_{0b} = s] \frac{(s-r)(1-\theta)}{n+1} \right\}_+ \right.$$

$$\left. - \left\{ \sum_{s=0} P[T_{0b} = s] \frac{(s-r)(1-\theta)}{n+1} \right\}_+ \right|$$

$$\leq \sum_{r=0}^{\lfloor n/2 \rfloor} P[T_{0b} = r] \sum_{s > \lfloor n/2 \rfloor} P[T_{0b} = s] \frac{(s-r)|1-\theta|}{n+1}$$

$$\leq |1-\theta| n^{-1} E(T_{0b} 1_{\{T_{0b} > n/2\}}) \leq 2|1-\theta| n^{-2} ET_{0b}^2, \quad (1.3)$$

and then by observing that

$$\sum_{r > \lfloor n/2 \rfloor} P[T_{0b} = r] \left\{ \sum_{s \geq 0} P[T_{0b} = s] \frac{(s-r)(1-\theta)}{n+1} \right\}$$

$$\leq n^{-1} |1-\theta| (ET_{0b} P[T_{0b} > n/2] + E(T_{0b} 1_{\{T_{0b} > n/2\}}))$$

$$\leq 4|1-\theta| n^{-2} ET_{0b}^2 \quad (1.4)$$

Combining the contributions of (1.2) –(1.3), we thus find that

$$|d_{TV}(L(C[1, b]), L(Z[1, b]))$$

$$-(n+1)^{-1} \sum_{r \geq 0} P[T_{0b} = r] \left\{ \sum_{s \geq 0} P[T_{0b} = s] (s-r)(1-\theta) \right\}_+$$

$$\leq \varepsilon_{\{7.8\}}(n, b)$$

$$= \frac{3}{\theta P_\theta[0,1]} \left\{ \varepsilon_{\{10.5(2)\}}(n/2, b) + 2n^{-1} ET_{0b} \varepsilon_{\{10.14\}}(n, b) \right\}$$

$$+ 2n^{-2} ET_{0b}^2 \left\{ 4 + 3|1-\theta| + \frac{24|1-\theta| \phi_{\{10.8\}}^*(n)}{\theta P_\theta[0,1]} \right\} \quad (1.5)$$

The quantity $\varepsilon_{\{7.8\}}(n, b)$ is seen to be of the order claimed under Conditions $(A_0), (D_1)$ and (B_{12}) , provided that $S(\infty) < \infty$; this supplementary condition can be removed if $\phi_{\{10.8\}}^*(n)$ is replaced by $\phi_{\{10.11\}}^*(n)$ in the definition of $\varepsilon_{\{7.8\}}(n, b)$, has the required order without the restriction on the r_i implied by assuming that $S(\infty) < \infty$. Finally, a direct calculation now shows that

$$\sum_{r \geq 0} P[T_{0b} = r] \left\{ \sum_{s \geq 0} P[T_{0b} = s] (s-r)(1-\theta) \right\}_+$$

$$= \frac{1}{2} |1-\theta| E|T_{0b} - ET_{0b}|$$

Example 1.0. Consider the point $O = (0, \dots, 0) \in \square^n$. For an arbitrary vector r , the coordinates of the point $x = O + r$ are equal to the respective coordinates of the vector $r : x = (x^1, \dots, x^n)$ and $r = (x^1, \dots, x^n)$. The vector r such as in the example is called the position vector or the radius vector of the point x . (Or, in greater detail: r is the radius-vector of x w.r.t an origin O). Points are frequently specified by their radius-vectors. This presupposes the choice of O as the “standard origin”. Let us summarize. We have considered \square^n and interpreted its elements in two ways: as points and as vectors. Hence we may say that we leading with the two copies of $\square^n : \square^n = \{\text{points}\}, \square^n = \{\text{vectors}\}$
 Operations with vectors: multiplication by a number, addition. Operations with points and vectors: adding a vector to a point (giving a point), subtracting two points (giving a vector). \square^n treated in this way is called an *n-dimensional affine space*. (An “abstract” affine space is a pair of sets, the set of points and the set of vectors so that the operations as above are defined axiomatically). Notice that vectors in an affine space are also known as “free vectors”. Intuitively, they are not fixed at points and “float freely” in space. From \square^n considered as an

affine space we can precede in two opposite directions: \mathbb{R}^n as an Euclidean space $\Leftarrow \mathbb{R}^n$ as an affine space $\Rightarrow \mathbb{R}^n$ as a manifold. Going to the left means introducing some extra structure which will make the geometry richer. Going to the right means forgetting about part of the affine structure; going further in this direction will lead us to the so-called “smooth (or differentiable) manifolds”. The theory of differential forms does not require any extra geometry. So our natural direction is to the right. The Euclidean structure, however, is useful for examples and applications. So let us say a few words about it:

Remark 1.0. *Euclidean geometry.* In \mathbb{R}^n considered as an affine space we can already do a good deal of geometry. For example, we can consider lines and planes, and quadric surfaces like an ellipsoid. However, we cannot discuss such things as “lengths”, “angles” or “areas” and “volumes”. To be able to do so, we have to introduce some more definitions, making \mathbb{R}^n a Euclidean space. Namely, we define the length of a vector $a = (a^1, \dots, a^n)$ to be

$$|a| := \sqrt{(a^1)^2 + \dots + (a^n)^2} \quad (1)$$

After that we can also define distances between points as follows:

$$d(A, B) := |\overline{AB}| \quad (2)$$

One can check that the distance so defined possesses natural properties that we expect: is it always non-negative and equals zero only for coinciding points; the distance from A to B is the same as that from B to A (symmetry); also, for three points, A, B and C, we have $d(A, B) \leq d(A, C) + d(C, B)$ (the “triangle inequality”). To define angles, we first introduce the scalar product of two vectors

$$(a, b) := a^1 b^1 + \dots + a^n b^n \quad (3)$$

Thus $|a| = \sqrt{(a, a)}$. The scalar product is also denote by dot: $a \cdot b = (a, b)$, and hence is often referred to as the “dot product”. Now, for nonzero vectors, we define the angle between them by the equality

$$\cos \alpha := \frac{(a, b)}{|a||b|} \quad (4)$$

The angle itself is defined up to an integral multiple of 2π . For this definition to be consistent we have to ensure that the r.h.s. of (4) does not exceed 1 by the absolute value. This follows from the inequality

$$(a, b)^2 \leq |a|^2 |b|^2 \quad (5)$$

known as the Cauchy–Bunyakovsky–Schwarz inequality (various combinations of these three names are applied in different books). One of the ways of proving (5) is to consider the scalar square of the linear combination $a + tb$, where $t \in \mathbb{R}$. As $(a + tb, a + tb) \geq 0$ is a quadratic polynomial in t which is never negative, its discriminant must be less or equal zero. Writing this explicitly yields (5). The triangle inequality for distances also follows from the inequality (5).

Example 1.1. Consider the function $f(x) = x^i$ (the i -th coordinate). The linear function dx^i (the differential of x^i) applied to an arbitrary vector h is simply h^i . From these examples follows that we can rewrite df as

$$df = \frac{\partial f}{\partial x^1} dx^1 + \dots + \frac{\partial f}{\partial x^n} dx^n, \quad (1)$$

which is the standard form. Once again: the partial derivatives in (1) are just the coefficients (depending on x); dx^1, dx^2, \dots are linear functions giving on an arbitrary vector h its coordinates h^1, h^2, \dots , respectively. Hence

$$df(x)(h) = \partial_{hf(x)} = \frac{\partial f}{\partial x^1} h^1 + \dots + \frac{\partial f}{\partial x^n} h^n, \quad (2)$$

Theorem 1.7. Suppose we have a parametrized curve $t \mapsto x(t)$ passing through $x_0 \in \mathbb{R}^n$ at $t = t_0$ and with the velocity vector $x(t_0) = v$. Then

$$\frac{df(x(t))}{dt}(t_0) = \partial_v f(x_0) = df(x_0)(v) \quad (1)$$

Proof. Indeed, consider a small increment of the parameter $t : t_0 \mapsto t_0 + \Delta t$, Where $\Delta t \mapsto 0$. On the other hand, we have $f(x_0 + h) - f(x_0) = df(x_0)(h) + \beta(h)|h|$ for an arbitrary vector h , where $\beta(h) \rightarrow 0$ when $h \rightarrow 0$. Combining it together, for the increment of $f(x(t))$ we obtain

$$\begin{aligned}
 & f(x(t_0 + \Delta t)) - f(x_0) + \beta(h)|h| \tag{3} \\
 & = df(x_0)(v.\Delta t + \alpha(\Delta t)\Delta t) \\
 & + \beta(v.\Delta t + \alpha(\Delta t)\Delta t).|v.\Delta t + \alpha(\Delta t)\Delta t| \\
 & = df(x_0)(v).\Delta t + \gamma(\Delta t)\Delta t
 \end{aligned}$$

Where $\beta(h) \rightarrow 0$ when $h \rightarrow 0$. We have $dF = (dF^1, \dots, dF^m)$ and

$$\begin{aligned}
 dF &= \frac{\partial F}{\partial x^1} dx^1 + \dots + \frac{\partial F}{\partial x^n} dx^n \\
 &= \begin{pmatrix} \frac{\partial F^1}{\partial x^1} & \dots & \frac{\partial F^1}{\partial x^n} \\ \dots & \dots & \dots \\ \frac{\partial F^m}{\partial x^1} & \dots & \frac{\partial F^m}{\partial x^n} \end{pmatrix} \begin{pmatrix} dx^1 \\ \dots \\ dx^n \end{pmatrix} \tag{4}
 \end{aligned}$$

For a certain $\gamma(\Delta t)$ such that $\gamma(\Delta t) \rightarrow 0$ when $\Delta t \rightarrow 0$ (we used the linearity of $df(x_0)$). By the definition, this means that the derivative of $f(x(t))$ at $t = t_0$ is exactly $df(x_0)(v)$. The statement of the theorem can be expressed by a simple formula:

$$\frac{df(x(t))}{dt} = \frac{\partial f}{\partial x^1} x^1 + \dots + \frac{\partial f}{\partial x^n} x^n \tag{2}$$

To calculate the value Of df at a point x_0 on a given vector v one can take an arbitrary curve passing Through x_0 at t_0 with v as the velocity vector at t_0 and calculate the usual derivative of $f(x(t))$ at $t = t_0$.

Theorem 1.8. For functions $f, g : U \rightarrow \mathbb{R}$, $U \subset \mathbb{R}^n$,

$$d(f + g) = df + dg \tag{1}$$

$$d(fg) = df.g + f.dg \tag{2}$$

Proof. Consider an arbitrary point x_0 and an arbitrary vector v stretching from it. Let a curve $x(t)$ be such that $x(t_0) = x_0$ and $x'(t_0) = v$. Hence

$$d(f + g)(x_0)(v) = \frac{d}{dt}(f(x(t)) + g(x(t)))$$

at $t = t_0$ and

$$d(fg)(x_0)(v) = \frac{d}{dt}(f(x(t))g(x(t)))$$

at $t = t_0$ Formulae (1) and (2) then immediately follow from the corresponding formulae for the usual derivative Now, almost without change the theory generalizes to functions taking values in \mathbb{R}^m instead of \mathbb{R} . The only difference is that now the differential of a map $F : U \rightarrow \mathbb{R}^m$ at a point x will be a linear function taking vectors in \mathbb{R}^n to vectors in \mathbb{R}^m (instead of \mathbb{R}). For an arbitrary vector $h \in \mathbb{R}^n$,

$$F(x+h) = F(x) + dF(x)(h)$$

In this matrix notation we have to write vectors as vector-columns.

Theorem 1.9. For an arbitrary parametrized curve $x(t)$ in \mathbb{R}^n , the differential of a map $F : U \rightarrow \mathbb{R}^m$ (where $U \subset \mathbb{R}^n$) maps the velocity vector $x(t)$ to the velocity vector of the curve $F(x(t))$ in \mathbb{R}^m :

$$\frac{dF(x(t))}{dt} = dF(x(t))(x'(t)) \tag{1}$$

Proof. By the definition of the velocity vector,

$$x(t + \Delta t) = x(t) + x'(t).\Delta t + \alpha(\Delta t)\Delta t \tag{2}$$

Where $\alpha(\Delta t) \rightarrow 0$ when $\Delta t \rightarrow 0$. By the definition of the differential,

$$F(x+h) = F(x) + dF(x)(h) + \beta(h)|h| \tag{3}$$

Where $\beta(h) \rightarrow 0$ when $h \rightarrow 0$. we obtain

$$F(x(t + \Delta t)) = F(x + \underbrace{x'(t).\Delta t + \alpha(\Delta t)\Delta t}_h)$$

$$= F(x) + dF(x)(x'(t)\Delta t + \alpha(\Delta t)\Delta t) +$$

$$\beta(x'(t)\Delta t + \alpha(\Delta t)\Delta t).|x'(t)\Delta t + \alpha(\Delta t)\Delta t|$$

$$= F(x) + dF(x)(x'(t)\Delta t + \gamma(\Delta t)\Delta t)$$

For some $\gamma(\Delta t) \rightarrow 0$ when $\Delta t \rightarrow 0$

This precisely means that $dF(x)x'(t)$ is the velocity vector of $F(x)$. As every vector attached to a point can be viewed as the velocity vector of some curve passing through this point, this theorem gives a clear geometric picture of dF as a linear map on vectors.

Theorem 1.10 Suppose we have two maps $F:U \rightarrow V$ and $G:V \rightarrow W$, where $U \subset \mathbb{R}^n, V \subset \mathbb{R}^m, W \subset \mathbb{R}^p$ (open domains). Let $F: x \mapsto y = F(x)$. Then the differential of the composite map $GoF:U \rightarrow W$ is the composition of the differentials of F and G :

$$d(GoF)(x) = dG(y)odF(x) \tag{4}$$

Proof. We can use the description of the differential. Consider a curve $x(t)$ in \mathbb{R}^n with the velocity vector \dot{x} . Basically, we need to know to which vector in \mathbb{R}^p it is taken by $d(GoF)$. the curve $(GoF)(x(t)) = G(F(x(t)))$. By the same theorem, it equals the image under dG of the Anycast Flow vector to the curve $F(x(t))$ in \mathbb{R}^m . Applying the theorem once again, we see that the velocity vector to the curve $F(x(t))$ is the image under dF of the vector $\dot{x}(t)$. Hence $d(GoF)(x) = dG(dF(x))$ for an arbitrary vector \dot{x} .

Corollary 1.0. If we denote coordinates in \mathbb{R}^n by (x^1, \dots, x^n) and in \mathbb{R}^m by (y^1, \dots, y^m) , and write

$$dF = \frac{\partial F}{\partial x^1} dx^1 + \dots + \frac{\partial F}{\partial x^n} dx^n \tag{1}$$

$$dG = \frac{\partial G}{\partial y^1} dy^1 + \dots + \frac{\partial G}{\partial y^m} dy^m, \tag{2}$$

Then the chain rule can be expressed as follows:

$$d(GoF) = \frac{\partial G}{\partial y^1} dF^1 + \dots + \frac{\partial G}{\partial y^m} dF^m, \tag{3}$$

Where dF^i are taken from (1). In other words, to get $d(GoF)$ we have to substitute into (2) the expression for $dy^i = dF^i$ from (3). This can also be expressed by the following matrix formula:

$$d(GoF) = \begin{pmatrix} \frac{\partial G^1}{\partial y^1} & \dots & \frac{\partial G^1}{\partial y^m} \\ \dots & \dots & \dots \\ \frac{\partial G^p}{\partial y^1} & \dots & \frac{\partial G^p}{\partial y^m} \end{pmatrix} \begin{pmatrix} \frac{\partial F^1}{\partial x^1} & \dots & \frac{\partial F^1}{\partial x^n} \\ \dots & \dots & \dots \\ \frac{\partial F^m}{\partial x^1} & \dots & \frac{\partial F^m}{\partial x^n} \end{pmatrix} \begin{pmatrix} dx^1 \\ \dots \\ dx^n \end{pmatrix} \tag{4}$$

i.e., if dG and dF are expressed by matrices of partial derivatives, then $d(GoF)$ is expressed by the product of these matrices. This is often written as

$$\begin{pmatrix} \frac{\partial z^1}{\partial x^1} & \dots & \frac{\partial z^1}{\partial x^n} \\ \dots & \dots & \dots \\ \frac{\partial z^p}{\partial x^1} & \dots & \frac{\partial z^p}{\partial x^n} \end{pmatrix} = \begin{pmatrix} \frac{\partial z^1}{\partial y^1} & \dots & \frac{\partial z^1}{\partial y^m} \\ \dots & \dots & \dots \\ \frac{\partial z^p}{\partial y^1} & \dots & \frac{\partial z^p}{\partial y^m} \end{pmatrix}$$

$$\begin{pmatrix} \frac{\partial y^1}{\partial x^1} & \dots & \frac{\partial y^1}{\partial x^n} \\ \dots & \dots & \dots \\ \frac{\partial y^m}{\partial x^1} & \dots & \frac{\partial y^m}{\partial x^n} \end{pmatrix}, \tag{5}$$

Or

$$\frac{\partial z^\mu}{\partial x^a} = \sum_{i=1}^m \frac{\partial z^\mu}{\partial y^i} \frac{\partial y^i}{\partial x^a}, \tag{6}$$

Where it is assumed that the dependence of $y \in \mathbb{R}^m$ on $x \in \mathbb{R}^n$ is given by the map F , the dependence of $z \in \mathbb{R}^p$ on $y \in \mathbb{R}^m$ is given by the map G , and the dependence of $z \in \mathbb{R}^p$ on $x \in \mathbb{R}^n$ is given by the composition GoF .

Definition 1.6. Consider an open domain $U \subset \mathbb{R}^n$. Consider also another copy of \mathbb{R}^n , denoted for distinction \mathbb{R}^n_y , with the standard coordinates $(y^1 \dots y^n)$. A system of coordinates in the open domain U is given by a map $F:V \rightarrow U$, where $V \subset \mathbb{R}^n_y$ is an open domain of \mathbb{R}^n_y , such that the following three conditions are satisfied:

- (1) F is smooth;
- (2) F is invertible;
- (3) $F^{-1}:U \rightarrow V$ is also smooth

The coordinates of a point $x \in U$ in this system are the standard coordinates of $F^{-1}(x) \in \mathbb{R}^n_y$

In other words,

$$F:(y^1 \dots, y^n) \mapsto x = x(y^1 \dots, y^n) \tag{1}$$

Here the variables $(y^1 \dots, y^n)$ are the “new” coordinates of the point x

Example 1.2. Consider a curve in \mathbb{R}^2 specified in polar coordinates as

$$x(t): r = r(t), \varphi = \varphi(t) \tag{1}$$

We can simply use the chain rule. The map $t \mapsto x(t)$ can be considered as the composition of the maps $t \mapsto (r(t), \varphi(t)), (r, \varphi) \mapsto x(r, \varphi)$. Then, by the chain rule, we have

$$\dot{x} = \frac{dx}{dt} = \frac{\partial x}{\partial r} \frac{dr}{dt} + \frac{\partial x}{\partial \varphi} \frac{d\varphi}{dt} = \frac{\partial x}{\partial r} \dot{r} + \frac{\partial x}{\partial \varphi} \dot{\varphi} \quad (2)$$

Here \dot{r} and $\dot{\varphi}$ are scalar coefficients depending on t , whence the partial derivatives $\frac{\partial x}{\partial r}, \frac{\partial x}{\partial \varphi}$ are vectors depending on point in \square^2 . We can compare this with the formula in the “standard” coordinates: $x = e_1 x + e_2 y$. Consider the vectors $\frac{\partial x}{\partial r}, \frac{\partial x}{\partial \varphi}$. Explicitly we have

$$\frac{\partial x}{\partial r} = (\cos \varphi, \sin \varphi) \quad (3)$$

$$\frac{\partial x}{\partial \varphi} = (-r \sin \varphi, r \cos \varphi) \quad (4)$$

From where it follows that these vectors make a basis at all points except for the origin (where $r = 0$). It is instructive to sketch a picture, drawing vectors corresponding to a point as starting from that point. Notice that $\frac{\partial x}{\partial r}, \frac{\partial x}{\partial \varphi}$ are, respectively, the velocity vectors for the curves $r \mapsto x(r, \varphi)$ ($\varphi = \varphi_0$ fixed) and $\varphi \mapsto x(r, \varphi)$ ($r = r_0$ fixed). We can conclude that for an arbitrary curve given in polar coordinates the velocity vector will have components $(\dot{r}, \dot{\varphi})$ if as a basis we take $e_r := \frac{\partial x}{\partial r}, e_\varphi := \frac{\partial x}{\partial \varphi}$:

$$\dot{x} = e_r \dot{r} + e_\varphi \dot{\varphi} \quad (5)$$

A characteristic feature of the basis e_r, e_φ is that it is not “constant” but depends on point. Vectors “stuck to points” when we consider curvilinear coordinates.

Proposition 1.3. The velocity vector has the same appearance in all coordinate systems.

Proof. Follows directly from the chain rule and the transformation law for the basis e_i . In particular, the elements of the basis $e_i = \frac{\partial x}{\partial x^i}$ (originally, a formal notation) can be understood directly as the velocity vectors of the coordinate lines $x^i \mapsto x(x^1, \dots, x^n)$ (all coordinates but x^i are fixed). Since we now know how to handle velocities

in arbitrary coordinates, the best way to treat the differential of a map $F: \square^n \rightarrow \square^m$ is by its action on the velocity vectors. By definition, we set

$$dF(x_0): \frac{dx(t)}{dt}(t_0) \mapsto \frac{dF(x(t))}{dt}(t_0) \quad (1)$$

Now $dF(x_0)$ is a linear map that takes vectors attached to a point $x_0 \in \square^n$ to vectors attached to the point $F(x) \in \square^m$

$$dF = \frac{\partial F}{\partial x^1} dx^1 + \dots + \frac{\partial F}{\partial x^n} dx^n$$

$$(e_1, \dots, e_m) \begin{pmatrix} \frac{\partial F^1}{\partial x^1} & \dots & \frac{\partial F^1}{\partial x^n} \\ \dots & \dots & \dots \\ \frac{\partial F^m}{\partial x^1} & \dots & \frac{\partial F^m}{\partial x^n} \end{pmatrix} \begin{pmatrix} dx^1 \\ \dots \\ dx^n \end{pmatrix}, \quad (2)$$

In particular, for the differential of a function we always have

$$df = \frac{\partial f}{\partial x^1} dx^1 + \dots + \frac{\partial f}{\partial x^n} dx^n, \quad (3)$$

Where x^i are arbitrary coordinates. The form of the differential does not change when we perform a change of coordinates.

Example 1.3 Consider a 1-form in \square^2 given in the standard coordinates:

$$A = -ydx + xdy$$

In the polar coordinates we will have $x = r \cos \varphi, y = r \sin \varphi$, hence

$$dx = \cos \varphi dr - r \sin \varphi d\varphi$$

$$dy = \sin \varphi dr + r \cos \varphi d\varphi$$

Substituting into A , we get

$$A = -r \sin \varphi (\cos \varphi dr - r \sin \varphi d\varphi) + r \cos \varphi (\sin \varphi dr + r \cos \varphi d\varphi)$$

$$= r^2 (\sin^2 \varphi + \cos^2 \varphi) d\varphi = r^2 d\varphi$$

Hence $A = r^2 d\varphi$ is the formula for A in the polar coordinates. In particular, we see that this is again a 1-form, a linear combination of the differentials of coordinates with functions as coefficients. Secondly, in a more conceptual way, we can define a 1-form in a domain U as a linear function on vectors at every point of U :

$$\omega(v) = \omega_1 v^1 + \dots + \omega_n v^n, \quad (1)$$

If $v = \sum e_i v^i$, where $e_i = \frac{\partial x}{\partial x^i}$. Recall that the differentials of functions were defined as linear functions on vectors (at every point), and

$dx^i(e_j) = dx^i \left(\frac{\partial x}{\partial x^j} \right) = \delta_j^i$ (2) at every point x .

Theorem 1.9. For arbitrary 1-form ω and path γ , the integral $\int_{\gamma} \omega$ does not change if we change parametrization of γ provide the orientation remains the same.

Proof: Consider $\left\langle \omega(x(t)), \frac{dx}{dt} \right\rangle$ and $\left\langle \omega(x(t(t'))), \frac{dx}{dt} \right\rangle$ As $\left\langle \omega(x(t(t'))), \frac{dx}{dt} \right\rangle = \left\langle \omega(x(t(t'))), \frac{dx}{dt} \right\rangle \cdot \frac{dt}{dt}$,

Let p be a rational prime and let $K = \mathbb{Q}(\zeta_p)$. We write ζ for ζ_p or this section. Recall that K has degree $\varphi(p) = p-1$ over \mathbb{Q} . We wish to show that $O_K = \mathbb{Z}[\zeta]$. Note that ζ is a root of $x^p - 1$, and thus is an algebraic integer; since O_K is a ring we have that $\mathbb{Z}[\zeta] \subseteq O_K$. We give a proof without assuming unique factorization of ideals. We begin with some norm and trace computations. Let j be an integer. If j is not divisible by p , then ζ^j is a primitive p^{th} root of unity, and thus its conjugates are $\zeta, \zeta^2, \dots, \zeta^{p-1}$. Therefore

$$Tr_{K/\mathbb{Q}}(\zeta^j) = \zeta + \zeta^2 + \dots + \zeta^{p-1} = \Phi_p(\zeta) - 1 = -1$$

If p does divide j , then $\zeta^j = 1$, so it has only the one conjugate 1, and $Tr_{K/\mathbb{Q}}(\zeta^j) = p-1$ By linearity of the trace, we find that

$$Tr_{K/\mathbb{Q}}(1-\zeta) = Tr_{K/\mathbb{Q}}(1-\zeta^2) = \dots = Tr_{K/\mathbb{Q}}(1-\zeta^{p-1}) = p$$

We also need to compute the norm of $1-\zeta$. For this, we use the factorization

$$x^{p-1} + x^{p-2} + \dots + 1 = \Phi_p(x) = (x-\zeta)(x-\zeta^2)\dots(x-\zeta^{p-1});$$

Plugging in $x=1$ shows that

$$p = (1-\zeta)(1-\zeta^2)\dots(1-\zeta^{p-1})$$

Since the $(1-\zeta^j)$ are the conjugates of $(1-\zeta)$, this shows that $N_{K/\mathbb{Q}}(1-\zeta) = p$ The key result

for determining the ring of integers O_K is the following.

LEMMA 1.9

$$(1-\zeta)O_K \cap \mathbb{Z} = p\mathbb{Z}$$

Proof. We saw above that p is a multiple of $(1-\zeta)$ in O_K , so the inclusion $(1-\zeta)O_K \cap \mathbb{Z} \supseteq p\mathbb{Z}$ is immediate. Suppose now that the inclusion is strict. Since $(1-\zeta)O_K \cap \mathbb{Z}$ is an ideal of \mathbb{Z} containing $p\mathbb{Z}$ and $p\mathbb{Z}$ is a maximal ideal of \mathbb{Z} , we must have $(1-\zeta)O_K \cap \mathbb{Z} = \mathbb{Z}$. Thus we can write

$$1 = \alpha(1-\zeta)$$

For some $\alpha \in O_K$. That is, $1-\zeta$ is a unit in O_K .

COROLLARY 1.1 For any $\alpha \in O_K$,

$$Tr_{K/\mathbb{Q}}((1-\zeta)\alpha) \in p\mathbb{Z}$$

PROOF. We have

$$Tr_{K/\mathbb{Q}}((1-\zeta)\alpha) = \sigma_1((1-\zeta)\alpha) + \dots + \sigma_{p-1}((1-\zeta)\alpha) = \sigma_1(1-\zeta)\sigma_1(\alpha) + \dots + \sigma_{p-1}(1-\zeta)\sigma_{p-1}(\alpha) = (1-\zeta)\sigma_1(\alpha) + \dots + (1-\zeta^{p-1})\sigma_{p-1}(\alpha)$$

Where the σ_i are the complex embeddings of K (which we are really viewing as automorphisms of K) with the usual ordering. Furthermore, $1-\zeta^j$ is a multiple of $1-\zeta$ in O_K for every $j \neq 0$. Thus

$Tr_{K/\mathbb{Q}}(\alpha(1-\zeta)) \in (1-\zeta)O_K$ Since the trace is also a rational integer.

PROPOSITION 1.4 Let p be a prime number and

let $K = \mathbb{Q}(\zeta_p)$ be the p^{th} cyclotomic field. Then

$$O_K = \mathbb{Z}[\zeta_p] \cong \mathbb{Z}[x]/(\Phi_p(x)); \quad \text{Thus}$$

$1, \zeta_p, \dots, \zeta_p^{p-2}$ is an integral basis for O_K .

PROOF. Let $\alpha \in O_K$ and write

$$\alpha = a_0 + a_1\zeta + \dots + a_{p-2}\zeta^{p-2} \quad \text{With } a_i \in \mathbb{Z}.$$

Then

$$\alpha(1-\zeta) = a_0(1-\zeta) + a_1(\zeta - \zeta^2) + \dots + a_{p-2}(\zeta^{p-2} - \zeta^{p-1})$$

By the linearity of the trace and our above calculations we find that $Tr_{K/\mathbb{Q}}(\alpha(1-\zeta)) = pa_0$

We also have

$$Tr_{K/\mathbb{Q}}(\alpha(1-\zeta)) \in p\mathbb{Z}, \quad \text{so } a_0 \in \mathbb{Z} \quad \text{Next}$$

consider the algebraic integer

$(\alpha - a_0)\zeta^{-1} = a_1 + a_2\zeta + \dots + a_{p-2}\zeta^{p-3}$; This is an algebraic integer since $\zeta^{-1} = \zeta^{p-1}$ is. The same argument as above shows that $a_1 \in \mathbb{Z}$, and continuing in this way we find that all of the a_i are in \mathbb{Z} . This completes the proof.

Example 1.4 Let $K = \mathbb{Q}$, then the local ring $\mathbb{Z}_{(p)}$ is simply the subring of \mathbb{Q} of rational numbers with denominator relatively prime to p . Note that this ring $\mathbb{Z}_{(p)}$ is not the ring \mathbb{Z}_p of p -adic integers; to get \mathbb{Z}_p one must complete $\mathbb{Z}_{(p)}$. The usefulness of $O_{K,p}$ comes from the fact that it has a particularly simple ideal structure. Let a be any proper ideal of $O_{K,p}$ and consider the ideal $a \cap O_K$ of O_K . We claim that $a = (a \cap O_K)O_{K,p}$; That is, that a is generated by the elements of a in $a \cap O_K$. It is clear from the definition of an ideal that $a \supseteq (a \cap O_K)O_{K,p}$. To prove the other inclusion, let α be any element of a . Then we can write $\alpha = \beta/\gamma$ where $\beta \in O_K$ and $\gamma \notin p$. In particular, $\beta \in a$ (since $\beta/\gamma \in a$ and a is an ideal), so $\beta \in O_K$ and $\gamma \notin p$. so $\beta \in a \cap O_K$. Since $1/\gamma \in O_{K,p}$, this implies that $\alpha = \beta/\gamma \in (a \cap O_K)O_{K,p}$, as claimed. We can use this fact to determine all of the ideals of $O_{K,p}$. Let a be any ideal of $O_{K,p}$ and consider the ideal factorization of $a \cap O_K$ in O_K . write it as $a \cap O_K = p^n b$ For some n and some ideal b , relatively prime to p . we claim first that $bO_{K,p} = O_{K,p}$. We now find that $a = (a \cap O_K)O_{K,p} = p^n bO_{K,p} = p^n O_{K,p}$. Since $bO_{K,p} = O_{K,p}$. Thus every ideal of $O_{K,p}$ has the form $p^n O_{K,p}$ for some n ; it follows immediately that $O_{K,p}$ is noetherian. It is also now clear that $p^n O_{K,p}$ is the unique non-zero prime ideal in $O_{K,p}$. Furthermore, the inclusion $O_K \hookrightarrow O_{K,p} / pO_{K,p}$. Since $pO_{K,p} \cap O_K = p$, this map is also surjection, since the residue class of $\alpha/\beta \in O_{K,p}$ (with $\alpha \in O_K$ and $\beta \notin p$) is the image of $\alpha\beta^{-1}$

in $O_{K/p}$, which makes sense since β is invertible in $O_{K/p}$. Thus the map is an isomorphism. In particular, it is now abundantly clear that every non-zero prime ideal of $O_{K,p}$ is maximal. To show that $O_{K,p}$ is a Dedekind domain, it remains to show that it is integrally closed in K . So let $\gamma \in K$ be a root of a polynomial with coefficients in $O_{K,p}$; write this polynomial as $x^m + \frac{\alpha_{m-1}}{\beta_{m-1}}x^{m-1} + \dots + \frac{\alpha_0}{\beta_0}$ With $\alpha_i \in O_K$ and $\beta_i \in O_{K-p}$. Set $\beta = \beta_0\beta_1\dots\beta_{m-1}$. Multiplying by β^m we find that $\beta\gamma$ is the root of a monic polynomial with coefficients in O_K . Thus $\beta\gamma \in O_K$; since $\beta \notin p$, we have $\beta\gamma/\beta = \gamma \in O_{K,p}$. Thus $O_{K,p}$ is integrally closed in K .

COROLLARY 1.2. Let K be a number field of degree n and let α be in O_K then

$$N'_{K/\mathbb{Q}}(\alpha O_K) = |N_{K/\mathbb{Q}}(\alpha)|$$

PROOF. We assume a bit more Galois theory than usual for this proof. Assume first that K/\mathbb{Q} is Galois. Let σ be an element of $Gal(K/\mathbb{Q})$. It is clear that $\sigma(O_K)/\sigma(\alpha) \cong O_{K/\alpha}$; since $\sigma(O_K) = O_K$, this shows that $N'_{K/\mathbb{Q}}(\sigma(\alpha)O_K) = N'_{K/\mathbb{Q}}(\alpha O_K)$. Taking the product over all $\sigma \in Gal(K/\mathbb{Q})$, we have $N'_{K/\mathbb{Q}}(N_{K/\mathbb{Q}}(\alpha)O_K) = N'_{K/\mathbb{Q}}(\alpha O_K)^n$. Since $N_{K/\mathbb{Q}}(\alpha)$ is a rational integer and O_K is a free \mathbb{Z} -module of rank n ,

$O_K / N_{K/\mathbb{Q}}(\alpha)O_K$ Will have order $N_{K/\mathbb{Q}}(\alpha)^n$; therefore

$$N'_{K/\mathbb{Q}}(N_{K/\mathbb{Q}}(\alpha)O_K) = N_{K/\mathbb{Q}}(\alpha O_K)^n$$

This completes the proof. In the general case, let L be the Galois closure of K and set $[L:K] = m$.

IV. RESULTS

A. Single channel

The channel with best indices was the one related to electrode 3B. In total 72 spike classes were found of which 49 removed because non-significative. Of the remaining 23 classes, 8 contained most of spikes found. Two of these classes (3 and 5) are

represented. Nevertheless they still are not suitable for the discrimination of different stimuli.

B. Combined channel

Indices fw, 3fw and fw described above have been evaluated for all combinations in the hypersphere. By visual inspection combinations with good ranking values for the three indices were chosen. The best one turned out to be i.e. the difference between signals from electrodes 1B and 3B (multiplied by a normalization factor). Among the classes found by the spike sorting algorithm with this pseudo-channel, classes 4 and 11 are the most discriminating ones. The improvement w.r.t. single channel in the discrimination of different stimuli. Different stimuli are still partially overlapping but a remarkable separation is present between two bigger categories: touch/pain and sensations. Obviously a larger number of experiments is needed to co validate this preliminary results.

V. DISCUSSION

A. Component signals

Combinations of signals gathered from different recording sites of the tLIFE increase separability of the stimuli. This improvement is qualitatively and quantified where fw,cl is reported together with the Davies-Boudin Index [21]. This index is related to the ratio between the intra-cluster spread and the inter-cluster distance, therefore a lower value means better separability. As the above mentioned classes are found in a combination of signals, it is interesting to know the shape of a combined signal as well as the one of its components. The class 11 found by the algorithm and the average signals recorded from electrodes 1B and 3B. It is worth noting that the spike recorded by electrode 1B is a delayed version of the one present in 3B. The same happens for class 4. Among the different combinations the one performing the difference between electrodes 3B and 1B is probably preferred because:

- signals coming from far sources (ECG, EMG, . . .) reach the two electrodes nearly simultaneously and thus are cancelled by the subtraction;
- signals coming from near sources, in particular from near axons, reach the two electrodes with a delay such that the negative wave of the spike reaches the second electrode while the first one is already recording the positive wave; the waves are therefore enhanced by subtraction.

B. Relationships between channels

The waves recorded by the four electrodes every time on the combined channel (3B-1B) a class 11 is recognized. In the first case it is clear how the electrodes see the action potential propagating

through the axon. In the second case the relative amplitude of the spikes may be misleading but a better inspection reveals that the same order (4B to 1B) is satisfied. These considerations are compatible with knowledge from neurophysiology. The time delay between the peaks detected from electrode 4B and 1B is about 0.1 ms. Considering a sensory nerve conduction velocity for the sciatic nerve of a rabbit [22] of about 80 m/s, the distance covered in this time span should be nearly 8 mm. This is not so far from the value of the distance between the conductive pads 4B and 1B of about 5 mm.

VI. CONCLUSION

One of the motivations of this work is a potential increase in the amount of efferent neural information gathered with multisite recoding. Even if the experiments have been carried out with afferent stimuli, results indicate that signals coming from more than one nerve fiber can be discriminated. In order to assess whether the same also apply to efferent signals, experiments with an adequate protocol will be carried on in the next future. This study proposes the use of information from different recording sites in order to enhance significant signal w.r.t. background. Multisite electrodes also increase the complexity of the afferent feedback the artificial device can give back to the user. As possible outcome for hand prosthesis control there is the possibility to increase the number of degrees of freedom the user can control and the number of sensations she/he can receive back while limiting the number of electrodes implanted. Considerations proposed by this paper are preliminary and need further investigations in order to have statistical evidences. Anyway they open questions that worth being investigated.

A. Authors and Affiliations

Dr Akash Singh is working with IBM Corporation as an IT Architect and has been designing Mission Critical System and Service Solutions; He has published papers in IEEE and other International Conferences and Journals.

He joined IBM in Jul 2003 as a IT Architect which conducts research and design of High Performance Smart Grid Services and Systems and design mission critical architecture for High Performance Computing Platform and Computational Intelligence and High Speed Communication systems. He is a member of IEEE (Institute for Electrical and Electronics Engineers), the AAI (Association for the Advancement of Artificial Intelligence) and the AACR (American Association for Cancer Research). He is the recipient of numerous awards from World Congress in Computer Science, Computer Engineering and Applied Computing 2010, 2011, and IP Multimedia System 2008 and Billing and Roaming 2008. He is active research in the field of Artificial Intelligence

and advancement in Medical Systems. He is in Industry for 18 Years where he performed various role to provide the Leadership in Information Technology and Cutting edge Technology.

REFERENCES

- [1] X. Navarro, T. B. Krueger, N. Lago, S. Micera, T. Stieglitz, and P. Dario, "A critical review of interfaces with the peripheral nervous system for the control of neuroprostheses and hybrid bionic systems," *J. Peripher. Nerv. Syst.*, vol. 10, pp. 229–258, Sep 2005.
- [2] G. R. M'uller-Putz, R. Scherer, G. Pfurtscheller, and R. Rupp, "EEGbased neuroprosthesis control: a step towards clinical practice," *Neurosci Lett*, vol. 382, no. 1-2, pp. 169–174, 2005.
- [3] M. A. Nicolelis, "Actions from thoughts," *Nature*, vol. 409, pp. 403–407, Jan 2001.
- [4] A. B. Schwartz, "Cortical neural prosthetics," *Annu Rev Neurosci*, vol. 27, pp. 487–507, 2004.
- [5] G. S. Dhillon, T. B. Krger, J. S. Sandhu, and K. W. Horch, "Effects of short-term training on sensory and motor function in severed nerves of long-term human amputees," *J Neurophysiol*, vol. 93, pp. 2625–2633, May 2005.
- [6] S. Micera, J. Carpaneto, M. Umilt`a, M. Rochat, L. Escola, V. Gallese, M. Carrozza, J. Krueger, G. Rizzolatti, and P. Dario, "Preliminary analysis of multi-channel recordings for the development of a high-level cortical neural prosthesis," in *2nd IEEE Int. Conf. Neural Eng. (NER 2005)*, pp. 136–139, 2005.
- [7] S. Micera, M. Carrozza, L. Beccai, F. Vecchi, and P. Dario, "Hybrid bionic systems for the replacement of hand function." Unpublished, 2005.
- [8] M. Zecca, S. Micera, M. Carrozza, and P. Dario, "Control of multifunctional prosthetic hands by processing the electromyographic signal," *Crit Rev Biomed Eng*, vol. 30, no. 4-6, pp. 459–485, 2002.
- [9] S. Roccella, M. Carrozza, G. Cappiello, P. Dario, J. Cabibihan, M. Zecca, H. Miwa, K. Itoh, and M. Marsumoto, "Design, fabrication and preliminary results of a novel anthropomorphic hand for humanoid robotics: Reh-1," in *IEEE/RSJ IROS Inter. Conf.*, vol. 1, pp. 266–271 vol.1, 2004.
- [10] T. Elbert, A. Sterr, H. Flor, B. Rockstroh, S. Knecht, C. Pantev, C. Wienbruch, and E. Taub, "Input-increase and input-decrease types of cortical reorganization after upper extremity amputation in humans," *Exp Brain Res*, vol. 117, pp. 161–164, Oct 1997.
- [11] G. L. Widener and P. D. Cheney, "Effects on muscle activity from microstimuli applied to somatosensory and motor cortex during voluntary movement in the monkey," *J Neurophysiol*, vol. 77, pp. 2446–65, May 1997.
- [12] M. Tarler and J. Mortimer, "Selective and independent activation of four motor fascicles using a four contact nerve-cuff electrode," *IEEE Trans Neur Sys Rehab Eng*, vol. 12, no. 2, pp. 251–257, 2004.
- [13] N. Lago, D. Ceballos, F. J. Rodriguez, T. Stieglitz, and X. Navarro, "Long term assessment of axonal regeneration through polyimide regenerative electrodes to interface the peripheral nerve," *Biomaterials*, vol. 26, pp. 2021–2031, May 2005.
- [14] K. Yoshida and R. B. Stein, "Characterization of signals and noise rejection with bipolar longitudinal intrafascicular electrodes," *IEEE Trans Biomed Eng*, vol. 46, pp. 226–234, Feb 1999.
- [15] S. M. Lawrence, G. S. Dhillon, W. Jensen, K. Yoshida, and K. W. Horch, "Acute peripheral nerve recording characteristics of polymerbased longitudinal intrafascicular electrodes," *IEEE Trans Neural Syst Rehabil Eng*, vol. 12, pp. 345–348, Sep 2004.
- [16] S. Bossi, S. Micera, A. Menciassi, L. Beccai, K. P. Hoffmann, K. P. Koch, and P. Dario, "On the actuation of thin film longitudinal intrafascicular electrodes." This conference.
- [17] K. P. Hoffmann and K. P. Koch, "Final report on design consideration of tLIFE2," tech. rep., IBMT, 2005.
- [18] G. S. Dhillon, S. M. Lawrence, D. T. Hutchinson, and K. W. Horch, "Residual function in peripheral nerve stumps of amputees: implications for neural control of artificial limbs," *J Hand Surg-AM*, vol. 29, pp. 605–18, Jul 2004.
- [19] A. Diedrich, W. Charoensuk, R. J. Brychta, A. C. Ertl, and R. Shiavi, "Analysis of raw microneurographic recordings based on wavelet denoising technique and classification algorithm: wavelet analysis in microneurography," *IEEE Trans Biomed Eng*, vol. 50, pp. 41–50, Jan 2003.
- [20] M. H. Ahn, S. Micera, K. Yoshida, M. C. Carrozza, and P. Dario, "Application of spike sorting techniques for chronic assessment of longitudinal intra-fascicular electrodes in neuroprosthetic and

- neurobotic systems,” J Neural Eng, vol. (accepted), 2005.
- [21] U. Maulik and S. Bandyopadhyay, “Performance evaluation of some clustering algorithms and validity indices,” Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 24, no. 12, pp. 1650–1654, 2002.
- [22] P. Schratzberger, D. H. Walter, K. Rittig, F. H. Bahlmann, R. Pola, C. Curry, M. Silver, J. G. Krainin, D. H. Weinberg, A. H. Ropper, and J. M. Isner, “Reversal of experimental diabetic neuropathy by VEGF gene transfer,” J Clin Invest, vol. 107, pp. 1083–1092, May 2001.

