Mathematical Foundations for Information Theory in Diffusion-Based Molecular Communication

Ya-Ping Hsieh and Ping-Cheng Yeh, Member, IEEE,

Abstract

Molecular communication emerges as a promising communication paradigm for nanotechnology. However, solid mathematical foundations for information-theoretic analysis of molecular communication have not yet been built. In particular, no one has ever proven that the channel coding theorem applies to molecular communication, and no relationship between information rate capacity (maximum mutual information) and code rate capacity (supremum achievable code rate) has been established. In this paper, we focus on a major sub-class of molecular communication – the diffusion-based molecular communication. We provide solid mathematical foundations for information theory in diffusion-based molecular communication by creating a general diffusion-based molecular channel model in measure-theoretic form and prove its channel coding theorems. Various equivalence relationships between statistical and operational definitions of channel capacity are also established, including the most classic information rate capacity and code rate capacity. As byproducts, we have shown that the diffusion-based molecular channel is with “asymptotically decreasing input memory and anticipation” and “\(d\)-continuous”. Other properties of diffusion-based molecular channel such as stationarity or ergodicity are also proven.

Index Terms

Molecular communication, diffusion process, diffusion-based molecular system, channel capacity, nanotechnology, \(d\)-continuous channel, asymptotically decreasing input memory and anticipation channel, permutation channel, cascade of channels.

I. INTRODUCTION

Molecular communication is a recently developed communication paradigm whose communication process involves “transmission and reception of information encoded in molecules” [1]. It is born in the study of nano-scale communication in nanonetworks [1] where the applicability of classical electromagnetic communication is limited by several constraints and a novel solution is called for. Inspired by the biological communication process such as the intra- and inter-cellular communication by cells [2] and the pheromone diffusion by insects [3], the researchers have created various message-carrying molecules and their corresponding receptors. Since the molecules are themselves at the nano-scale, the difficulty of nano-scale communication is solved by building up communication media between the transmitter and the receptor. Moreover, since the major potential application of nanonetworks is implemented in the organisms body (e.g., organ monitoring in human body), the compatibility of the bioinspired communication process makes it a perfect choice to consider the encoding, transmission, and decoding of messages in molecules. Excited by the reasons above (and beyond), the researchers have treated the molecular communication as one of the mainstream subjects of nanotechnology nowadays.

Among the various proposed system blue maps for molecular communication, a specific class of system called the “diffusion-based molecular system” draws lots of interest due to the universality of mass transport phenomena in molecular communication. The mass transport phenomena refer to the propagation of encoded molecules in the communication media. In most cases, the communication media of molecular communication are modeled as fluid. As is well-known, the motion of molecules in fluid media is governed by the “diffusion process”. The universality of mass transport phenomena not only make the study of diffusion-based system natural, but at the same time guarantee the widest possible generality of research results. To this end, most efforts in molecular communication are devoted to diffusion-based systems, both in practical system design and information-theoretic analysis point of view. For example, for the practical system design, the physical phenomena of bacteria chemotaxis, pheromone diffusion [4], or calcium diffusion [5] are adopted, and there are many existing systems operating on these phenomena such as [6], [7], and [8]. The information-theoretic analysis of diffusion-based molecular system are also conducted in [9], [10], and [11].

Despite of this much effort for diffusion-based molecular communication, two important things are still lacking. First, an unified channel model for diffusion-based molecular communication is missing. The existing works on information-theoretic analysis tend to be system-dependent; that is, they are treating different kinds of diffusion-based systems independently and giving their own capacity analysis. So far, the most general result concerning the information rate capacity of diffusion-based molecular communication is probably [11] where the authors have cleverly utilized the thermodynamics to derive the information rate capacity in closed form, but the result is only valid for receiver with Poisson noise. Second, and the more important one, no mathematical foundations have been put down for information theory in diffusion-based molecular communication. In particular, the channel coding theorem is not proven for diffusion-based systems. To state more directly, no one has ever shown that, for...
the diffusion-based molecular channel, the information rate capacity (maximum mutual information) is equal to the code rate capacity (supremum achievable code rate), where the former is a system statistic of mathematical importance and the latter is the real practical concern. Furthermore, the diffusion-based molecular channels exhibit non-classical randomness (which is explained later in Section IV.A) and no existing channel model apply to diffusion-based molecular channel. Therefore, the lacking of proof for equivalence between the information rate capacity and code rate capacity renders the purpose of calculating information rate capacity ambiguous, or at least in a shaky situation.

This paper aims at solving the above two problems once and for all. Let us first put molecular communication aside for a moment and recall the history of information theory. Ever since the advent of the paper [12] by Shannon in 1948, the “Channel Capacity” has been the primary subject of every communication systems. In particular, the way that Shannon intervenes the information-theoretic and coding-theoretic quantities for discrete memoryless channels is the one that communication engineers imitate when treating the communication system under consideration. Despite its great novelty and ingenuity, a complete and rigorous mathematical setting for information theory is not laid down until a series of papers by McMillan [13], Feinstein [14], and finally Khinchin [15], where the definition of “finite memory channel without anticipation” is made precise and for such channels the equivalence between the information rate capacity and code rate capacity is established. A key step of [15] is the measure-theoretic formulation for sources and channels. Khinchin noticed that except for some simple classes of channel (e.g., i.i.d., Markov, ...), the mathematical formulations of sources and channels are most conveniently made in the measure-theoretic form to provide rigorousness and applicability. Later, works in [15] are generalized by many others (e.g., [16], [17], [18], ...) to include classes of channels other than finite memory channel without anticipation, all under the same proof structure. It is now a communication engineers’ consensus that the measure-theoretic formulations of source and channel have struck a perfect balance between the mathematical rigorousness of information theory and the applicability thereof to practical communication systems. Therefore, for any communication system, once its channel abstraction is made in the measure-theoretic form and the corresponding capacity theorems are derived, then a solid mathematical foundation is laid down and applicability of information theory to the system is guaranteed.

In this paper, we shall follow the path of Khinchin [15] to provide the mathematical foundations for information theory in diffusion-based molecular communication. Fortunately, there are already many building blocks from the works of predecessors [16], [17], and [19]. From these works, the two crucial concepts of “channels with asymptotically decreasing input memory and anticipation” and “d-continuous channels” will be used heavily in our paper. We will give a channel model for diffusion-based molecular communication in the most rigorous language, namely the measure-theoretic one. The channel model we create captures the essential features of all existing diffusion-based molecular systems and all diffusion-based molecular systems to come, thus allowing our results the maximum possible generality. For our channel, we first prove its d-continuity and then utilize the d-continuity to establish various equivalence relationships between the statistical and operational definitions of channel capacity, including the equivalence of information rate capacity and the code rate capacity. In particular, the channel coding theorems for diffusion-based molecular channel is given. A solid foundation is therefore laid down and we can use the usual sense of “channel capacity” without worry thereafter.

The rest of paper is organized as follows. We state the essential terminologies and notations in Section II. Section III introduces “channels with asymptotically decreasing input memory and anticipation” and “d-continuous channels” as well as their properties for our use. Section IV is the main section in which we give the definition of diffusion-based molecular channel and prove capacity theorems, along with some discussions. Finally, we conclude this paper in Section V.

II. Preliminaries

A. Sources

We begin by setting up terminology and notation for sources. If a set $A$ is finite, the symbol $A^\infty$ will denote the set of all doubly infinite sequences $x = (\cdots, x_{-2}, x_{-1}, x_0, x_1, x_2, \cdots)$, $x_i \in A$ for all $i$. The notation $x^m_n$ denotes the finite sequence $(x_m, x_{m+1}, \cdots, x_n)$ and $A^m_n$ stands for the set of all such sequences. Given a sequence $a^m_n \in A^m_n$, there corresponds a cylinder set (or rectangle set):

$$C(a^m_n) = \{ x \in A^\infty | x_i = a_i \text{ for } m \leq i \leq n \}.$$ 

The Borel field generated by all cylinder sets in $A^\infty$ will be denoted by $B_A$.

A source is a probability measure $\mu$ on the measurable space $(A^\infty, B_A)$ and $A$ is called the alphabet of the source. The probability measure $\mu$ induces a sequence of random variables $\{X_n| n = -\infty, \cdots, \infty\}$ on the probability space $(A^\infty, B_A, \mu)$ by the formula $X_n(x) = x_n$ for all $x \in A^\infty$. For integers $m$ and $n$ define $B_A(m, m + n)$ as the Borel field generated by random variables $(X_m, X_{m+1}, \cdots, X_{m+n})$ and we allow $m = -\infty$ and $n = \infty$. The induced sequence $\{X_n\}_n$ is viewed as the transmitted signal for each time $n$, and $B_A(m, m + n)$ represents all possible events in time $m$ to $m + n$.

Besides $\{X_n\}_n$, $\mu$ also defines a probability measure $\mu^m_n$ on $A^m_n$ by the formula

$$\mu^m_n(a^m_n) = \mu(C(a^m_n)),$$ 

where $a^m_n \in A^m_n$. When $m = 0$, $\mu^m_n$ is abbreviated $\mu^n$. Whenever we need to emphasize the alphabet or the induced random variables, we will also use the notation $[A, \mu]$ or $[A, \mu, X]$ to denote a source.
The (left) shift operator $T$ on $A^\mathbb{Z}$ is defined by $(Tx)_n = x_{n+1}$, where $(Tx)_n$ is the element at the $n$th position. A source $\mu$ is said to be stationary if
$$\mu(F) = \mu(TF) \equiv \mu(T^{-1}F), \quad F \in \mathcal{B}_A.$$  

A source is $n$-stationary for some positive integer $n$ if $\mu(T^nF) = \mu(F)$ for all $F \in \mathcal{B}_A$. In other words, $\mu$ is stationary if it is shift-invariant with respect to all events, and it is $n$-stationary if it is $n$-times shift-invariant with respect to all events. Obviously stationarity implies $n$-stationarity. If $\mu$ is $n$-stationary for some $n$, we say that $\mu$ is block stationary.

A source $\mu$ is ergodic if for every $F \in \mathcal{B}_A$ such that $TF = F$, $\mu(F)$ is either 0 or 1. An important property of the ergodic sources is the following:

**Theorem 1.** For a given source $[A,\mu]$, denote the characteristic function of the set $F \in \mathcal{B}_A$ by $\chi_F(\cdot)$. Then, we have for all $F \in \mathcal{B}_A$
$$\lim_{n \to \infty} \frac{1}{n} \sum_{k=0}^{n-1} \chi_F(T^kx) = \mu(F) \quad a.e.,$$  

if and only if for every $F$ such that $TF = F$, $\mu(F)$ is either 0 or 1.

**Proof:** The necessity is provided by the well-known “ergodic theorem” of Birkhoff and the sufficiency is a direct verification of the definition. For complete proof, see, e.g., [13].

The summation appeared in the theorem represents the “ensemble mean”. **Theorem 1** therefore states that the ergodic sources are those whose features can be approximated well by ensemble statistics on observable samples.

**B. Channels**

A discrete channel is characterized by an input alphabet $A$, an output alphabet $B$, and a set of probability measures $\{ \nu_x \}_x$ on $(B^\mathbb{Z}_\infty, \mathcal{B}_B)$. The probability measure $\nu_x$ is determined for each $x \in A^\mathbb{Z}_\infty$ such that for each $F \in \mathcal{B}_B$ the mapping $x \to \nu_x(F)$ is $\mathcal{B}_A$-measurable. Each $\nu_x$ is recognized as the output distribution conditioning on the input $x$. We shall refer $[A,\nu,B]$ to such structure and say that $[A,\nu,B]$ is a channel. The channel is stationary if for every $x \in A^\mathbb{Z}_\infty$ and $F \in \mathcal{B}_B$ we have
$$\nu_x(F) = \nu_{Tx}(TF).$$

Now, consider the case of connecting a source $[A,\mu]$ to a channel $[A,\nu,B]$. We are naturally led to consider the probability measure $\nu \mu$ on the product space $((A \times B)^\mathbb{Z}_\infty, \mathcal{B}_{A \times B})$ characterized by
$$\nu \mu(F \times G) = \int_F \nu_x(G) d\mu(x), \quad F \in \mathcal{B}_A, \ G \in \mathcal{B}_B.$$  

The event $F \times G$ is interpreted as “source emits event $F$ and the channel output receives $G$”. If we are interested in the output process, we shall consider the probability measure $\overline{\nu \mu}$ on the output space $(B^\mathbb{Z}_\infty, \mathcal{B}_B)$:
$$\overline{\nu \mu}(G) = \mu(A^\mathbb{Z}_\infty \times G), \quad G \in \mathcal{B}_B.$$  

The sequence of random variables induced by $\overline{\nu \mu}$ on $(B^\mathbb{Z}_\infty, \mathcal{B}_B)$ will be denoted by $\{Y_n\}_n$. Elementary analysis shows that if $[A,\mu]$ and $[A,\nu,B]$ are both stationary, then so is $\nu \mu$ and $\overline{\nu \mu}$.

In this paper we will encounter the “cascade” of channels. Suppose that we are given two channels $[A,\sigma,Q]$ and $[Q,\eta,B]$. If we have these two channels in cascade, the overall channel $[A,\nu,B]$ is described by
$$\nu_x(F) = \int_{Q^\mathbb{Z}_\infty} \eta_q(F) d\sigma_x(q).$$

Another important notion of channel is the ergodicity. The channel $\nu$ is ergodic if for any input sequence $x$, $\nu_x$ is ergodic. The following is an useful criterion for examining the ergodicity of a channel:

**Theorem 2** (Strongly Mixing and Ergodicity). A stationary channel $[A,\nu,B]$ is said to be strongly mixing if for any input sequence $x$ and any two cylinders $F_1, F_2 \in \mathcal{B}_B$, we have
$$\lim_{n \to \infty} \left| \nu_x(T^{k}F_1 \cap F_2) - \nu_x(T^{k}F_1) \nu_x(F_2) \right| \to 0$$  

where $T$ is the time shift operator. If a channel is strongly mixing, then it is ergodic.

**Proof:** See [16].

Intuitively speaking, a channel is strongly mixing if for any two events separated by a long time at the output, the two events are “almost” independent, regardless of the input.
C. Information-Theoretic and Coding-Theoretic Quantities

We have seen that the source $\mu$ can be viewed as a sequence of random variables $\{X_n\}_n$. Similarly, we can view $\nu\nu$ as $\{Y_n\}_n$ and $\mu\nu$ as $\{X_n, Y_n\}_n$. It is well-known that if the processes represented by these sequences of random variables are stationary then their entropy rates exist. Since we shall only consider stationary ergodic sources and stationary channels in this paper, we are free to write

$$H(\mu) = H(X) = \lim_{N \to \infty} \frac{H(X_1, X_2, \ldots, X_N)}{N}$$

$$H(\nu\nu) = H(Y) = \lim_{N \to \infty} \frac{H(Y_1, Y_2, \ldots, Y_N)}{N}$$

$$H(\mu\nu) = H(X, Y) = \lim_{N \to \infty} \frac{H((X_1, Y_1), (X_2, Y_2), \ldots, (X_N, Y_N))}{N}.$$  

The mutual information rate between the input and output is defined as

$$I(\mu\nu) = H(\mu) + H(\nu\nu) - H(\mu\nu)$$

or, equivalently,

$$I(X; Y) = H(X) + H(Y) - H(X, Y).$$

In the rest of this paper we shall refer to these quantities interchangeably in their measure forms and random variable forms.

There are many definitions of channel capacity. In the following we state and itemize them for ease of reference. See [17], [18], and [19] for detail descriptions of these channel capacities.

Given a channel $[A, \nu, B]$, there are several choices of source which we can extremizing the mutual information over. The most common ones are the following:

- The ergodic capacity

  $$C_e = \sup_{\text{stationary and ergodic } [A, \mu]} I(\mu\nu),$$

- The stationary capacity

  $$C_s = \sup_{\text{stationary } [A, \mu]} I(\mu\nu),$$

and

- The block stationary capacity

  $$C = \sup_{n} \sup_{\text{n-stationary } [A, \mu]} I(\mu\nu).$$

We now state coding-theoretic terminologies. A blocklength $n$ channel block code $\mathcal{E}$ for a noisy channel $[A, \nu, B]$ is a collection of $|\mathcal{E}| = M$ distinct codewords $w_i \in A^n$ and $M$ disjoint decoding sets $\Gamma_i \in B_B(0, n)$ for each $i$. The rate $R$ of a code is $R = \frac{1}{n} \log M$. A code $\mathcal{E} = \{w_i, \Gamma_i | i = 1, 2, \cdots, M\}$ has probability error $\lambda$ if

$$\max_{1 \leq i \leq M} \sup_{x \in c(w_i)} \nu_x^n(\Gamma_i^c) \leq \lambda$$

where $\Gamma_i^c$ is the complement of $\Gamma_i$. Such a channel block code is called an $(M, n, \lambda)$ channel code.

We say $R$ is a permissible transmission rate if there exist $(< 2^{nR}, n, \epsilon_n)$ channel codes such that $\epsilon_n \to 0$ as $n \to \infty$. The operational channel block coding capacity $C_{cb}$ is defined to be the supreme of all permissible rate:

$$C_{cb} = \sup_{\text{R permissible}} R.$$  

An alternate operational definition of capacity, the operational source/channel block coding capacity $C_{scb}$, is defined as follows. We consider the transmission of an ergodic source $[G, \tau, U]$ over the channel $[A, \nu, B]$. Define a blocklength $n$ source/channel block code as a pair of mappings $\gamma_n : G^n \to A^n$ and $\psi_n : B^n \to G^n$. The $\gamma_n$ is called the encoder and $\psi_n$ the decoder. The block encoder $\gamma_n$ implements a mapping on infinite sequences $\gamma : G^{\infty} \to A^{\infty}$ defined by $\gamma(u) = (\cdots, \gamma_n(u_{-n}, \cdots, u_1), \gamma_n(u_0, \cdots, u_{n-1}), \cdots)$. All such encoded sequences can be viewed as another channel input process $[A, \tau \gamma^{-1}]$ characterized by $\tau \gamma^{-1}(F) = \tau(\gamma^{-1}(F))$ for all $F \in B_A$. The block error probability for the code is

$$P_e = Pr(\psi_n(Y^n) \neq U^n)$$
where $Y^n$ is the random variable induced at the channel output, or, presented in the measure from,

$$P_c = 1 - P_e = \int \nu_{\gamma(u)}^{-1}(U^n(u))d\tau(u).$$

A source/channel code of blocklength $n$ and of probability error $P_c$ is called an $(n, P_e)$ source/channel code.

A source $[G, \tau]$ is said to be admissible if there exist $(n, P_{e,n})$ source/channel codes for the source such that $P_{e,n} \to 0$ as $n \to \infty$. The operational source/channel block coding capacity $C_{scb}$ is defined as the supreme of the entropy over all admissible stationary ergodic sources:

- The operational source/channel block coding capacity

$$C_{scb} = \sup_{\text{admissible } [G, \tau]} H(\tau).$$

The last operational capacity definition concerns another function of samples defined over input/output alphabets. The $n$th order sample mutual information $i_n(x^n, y^n)$ is defined by

$$i_n(x^n, y^n) = \frac{1}{n} \log \frac{\mu^n(x^n, y^n)}{\mu^n(x^n)\mu^n(y^n)}.$$

If $\mu \nu$ is stationary then there exist a measurable shift-invariant nonnegative bounded function $i(x, y)$ such that

$$\lim_{n \to \infty} i_n(X^n(x), Y^n(y)) = i(x, y)$$

with convergence in $L_1(\mu \nu)$ and

$$E_{\mu \nu}i = \int i(x, y)d\mu \nu(x, y) = I(\mu \nu).$$

If, furthermore, $\mu \nu$ is ergodic, then the Shannon-McMiliam Theorem states that $i(x, y) = I(\mu \nu)$ $\mu \nu$-almost everywhere. Therefore, for stationary ergodic sources and channels the $n$th order sample mutual information $i_n(x^n, y^n)$ is a good approximation of the “true” mutual information $I(\mu \nu)$ provided $n$ is large enough. Define for a stationary channel $\nu$ and for $\lambda \in (0, 1)$ the quantile

$$C^*(\lambda) = \sup_\mu \sup \{r \mid \mu \nu(i \leq r) < \lambda\}$$

where $\mu \nu(i \leq r) = \mu \nu(\{(x, y) \mid i(x, y) \leq r\})$ and the outer supreme is taken over all block stationary input process $[A, \mu]$. Our last operational capacity definition, the information quantile capacity $C^*$, is defined by

- The information quantile capacity

$$C^* = \lim_{\lambda \to 0} C^*(\lambda).$$

The relation between all these capacities (namely, $C_e, C_s, C, C_{scb}, C_{scb}$, and $C^*$) will be given in Section III, where we need the notion of $d$-continuity to unify these concepts.

III. THE ADIMA CHANNEL AND THE $\bar{d}$-DISTANCE

A. ADIMA Channel

A channel $\nu$ is said to have asymptotically decreasing input memory if given $\epsilon > 0$ there is an integer $m(\epsilon)$ such that, for any $n$ and any output event $F \in B_B(n, \infty)$,

$$|\nu_x(F) - \nu_{x'}(F)| \leq \epsilon$$

whenever $x_i = x'_i$ for $i \geq n - m$. A channel $\nu$ is said to have asymptotically decreasing input anticipation if given $\epsilon > 0$ there is an integer $a(\epsilon)$ such that for any $n$ and any output event $F \in B_B(-\infty, n)$,

$$|\nu_x(F) - \nu_{x'}(F)| \leq \epsilon$$

whenever $x_i = x'_i$ for $i \leq n + a$. If a channel has both asymptotically decreasing input memory and input anticipation then we call such channels the ADIMA (asymptotically decreasing input memory and anticipation) channels or channels with ADIMA. Therefore, a channel $\nu$ with ADIMA is one for which given $\epsilon > 0$, there exist integers $m(\epsilon)$ and $a(\epsilon)$ such that for all $k, n$ and all $F \in B_B(k, k + n)$ we have

$$|\nu_x(F) - \nu_{x'}(F)| \leq \epsilon$$

whenever $x_i = x'_i$, $k - m \leq i \leq k + n + a$.

Intuitively speaking, a channel has asymptotically decreasing input memory if for any two input sequences $x$ and $x'$, the conditional channel output distributions $\nu_x$ and $\nu_{x'}$ in the interval $(y_n, y_{n+1}, \cdots)$ are “close” provided the two input sequences coincide on the interval $(x_{n-m}, x_{n-m+1}, \cdots)$. Similar interpretation works for channel with asymptotically decreasing input
anticipation. The measure of closeness can be made precise in the language of the variational distance. Given two probability measures \( \nu^n_x \) and \( \nu^n_{x'} \) on \( (B^n, \mathcal{B}(0, n)) \), the variational distance between the measures is defined by
\[
v_n(\nu^n_x, \nu^n_{x'}) = \sup_{G \in \mathcal{B}(0, n)} |\nu^n_x(G) - \nu^n_{x'}(G)|.
\]
If we consider stationary channels only (so that the definition of ADIMA can be made to require having only all \( F \in \mathcal{B}_B(0, n) \) with the desired property, not with all \( F \in \mathcal{B}_B(k, k + n) \) for all \( k \)), then we can rephrase the definition of the ADIMA channel by saying that a stationary channel is with ADIMA if, given \( \epsilon > 0 \), there are integers \( m(\epsilon) \) and \( a(\epsilon) \) such that for all \( n \),
\[
v_n(\nu^n_x, \nu^n_{x'}) \leq \epsilon
\]
whenever \( x_i = x'_i, -m \leq x \leq n + a \).

B. \( \bar{d} \)-Distance and \( \bar{d} \)-Continuity

Given two probability measures \( \nu^n_x \) and \( \nu^n_{x'} \) on \( (B^n, \mathcal{B}(0, n)) \), let \( \mathcal{P}(\nu^n_x, \nu^n_{x'}) \) denote the set of all joint probability measures \( p^n \) on \( (B^n \times B^n, \mathcal{B}(0, n) \times \mathcal{B}(0, n)) \) satisfying the property that for all \( G \in \mathcal{B}_B(0, n) \),
\[
p^n(G \times B^n) = \nu^n_x(G)
\]
and
\[
p^n(B^n \times G) = \nu^n_{x'}(G).
\]
In other words, \( p^n \) has \( \nu^n_x \) and \( \nu^n_{x'} \) as marginals. Define the coordinate functions \( U_i : B^n \times B^n \rightarrow B \) and \( W_i : B^n \times B^n \rightarrow B \), \( i, = 0, 1, \ldots, n - 1 \) by
\[
U_i(u^n, w^n) = u_i,
\]
\[
W_i(u^n, w^n) = w_i.
\]
Let \( d_H(a, b) = \begin{cases} 1, & a \neq b \\ 0, & a = b \end{cases} \) be the Hamming distance and let \( \delta_n \) to be the \( n \)th order normalized Hamming distance
\[
\delta_n(u^n, w^n) = \frac{1}{n} \sum_{i=0}^{n-1} d_H(u_i, w_i).
\]
The \( n \)th order \( \bar{d} \)-distance between \( \nu^n_x \) and \( \nu^n_{x'} \), is defined as
\[
\bar{d}_n(\nu^n_x, \nu^n_{x'}) = \inf_{p \in \mathcal{P}(\nu^n_x, \nu^n_{x'})} E_p \delta_n(U^n, W^n)
\]
\[
= \inf_{p \in \mathcal{P}(\nu^n_x, \nu^n_{x'})} \frac{1}{n} \sum_{i=0}^{n-1} p(U_i \neq W_i).
\]
A channel \( \nu \) is \( \bar{d} \)-continuous if given \( \epsilon > 0 \) there is an \( n_0 \) such that for \( n \geq n_0 \) we have \( \bar{d}_n(\nu^n_x, \nu^n_{x'}) \leq \epsilon \) whenever \( x_i = x'_i, i = 0, 1, \ldots, n - 1 \). Equivalently, \( \nu \) is \( \bar{d} \)-continuous if
\[
\limsup_{n \to \infty} \sup_{a^n \in A^n} \sup_{x, x' \in \mathcal{C}(a^n)} \bar{d}_n(\nu^n_x, \nu^n_{x'}) = 0.
\]

C. Properties of \( \bar{d} \)-Continuous Channel

Here we list several important properties of \( \bar{d} \)-continuous channel. We begin by establishing the relation between the ADIMA channel and \( \bar{d} \)-continuous channel.

**Theorem 3** (ADIMA Channel and \( \bar{d} \)-Continuity). A channel \( \nu \) is strongly \( d \)-continuous if given \( \epsilon > 0 \) there are positive integers \( m(\epsilon) \) and \( a(\epsilon) \) such that for all \( n \), \( \bar{d}_n(\nu^n_x, \nu^n_{x'}) \leq \epsilon \) whenever \( x_i = x'_i, -m \leq i \leq n + a \). An ADIMA channel is strongly \( d \)-continuous. A strongly \( d \)-continuous channel is \( \bar{d} \)-continuous.

**Proof:** See [17].

Next, we summarize information-theoretic results. Recall the following notions:
\[
C_{cb} \quad \text{Operational channel block coding capacity.}
\]
\[
C_{sch} \quad \text{Operational source/channel block coding capacity.}
\]
\[
C^* \quad \text{Information quantile capacity.}
\]
\[
C_e \quad \text{Ergodic capacity.}
\]
\[
C_s \quad \text{Stationary capacity.}
\]
\[
C \quad \text{Block stationary capacity.}
\]
Theorem 4. a) For stationary channels we have
\[ C = C_s = C_e. \]
Hence, for stationary channels, we can simply call \( C = C_s = C_e \) the information rate capacity (or transmission rate capacity or Shannon capacity).

b) If a channel is stationary and \( \bar{d} \)-continuous then
\[ C \geq C^* = C_{sch} = C_{ch}. \]

c) Let \( \nu \) be a discrete stationary \( \bar{d} \)-continuous channel. If \( R < C^* \) and \( \epsilon > 0 \), then for sufficiently large \( n_0 \) there exist \((2^{nR}, n, \epsilon)\) block codes for all \( n \geq n_0 \). If \( R > C^* \) there exists an \( \epsilon_{\min} > 0 \) such that there do not exist \((2^{nR}, n, \epsilon)\) block code for any \( \epsilon < \epsilon_{\min} \).

d) Let \( \nu \) be a discrete stationary \( \bar{d} \)-continuous channel and \( \mu \) a discrete stationary ergodic source. If \( H(\mu) < C^* \), then \( \mu \) is admissible. If \( H(\mu) > C^* \), then \( \mu \) is not admissible.

e) If, in addition, \( \nu \) is also ergodic in b), c), and d), then \( C = C^* \).

Proof: See [17].

Theorem 4 lists the most important channel coding theorems for discrete stationary \( \bar{d} \)-continuous channels. For a discrete stationary \( \bar{d} \)-continuous channel Theorem 4.c) says that if we transmit message at a rate \( R < C^* \), then \( R \) can be achieved by some block codes with arbitrarily small block error probability; conversely, if we transmit at a rate \( R > C^* \), then the block error probability is always bounded away from zero. Similarly, Theorem 4.d) says that, for a discrete stationary \( \bar{d} \)-continuous channel and any discrete stationary ergodic source \( \mu \), if \( H(\mu) < C^* \), then \( \mu \) can be transmitted via block coding with arbitrarily small block error probability; conversely, if \( H(\mu) > C^* \), then no such block code exists. The contents of Theorem 4.c) and Theorem 4.d) therefore collectively tell us that \( C^* \) is the ultimate limitation of the system performance over the given channel, where the performance is measured in terms of the maximal code rate with vanishing block error probability. Theorem 4.e) says that if, in addition, \( \nu \) is also ergodic, then the Shannon capacity \( C \) equals \( C^* \).

The last property we need for \( \bar{d} \)-continuous channel is its preservation under the \( \bar{d} \)-limit [19]:

Theorem 5. The \( \bar{d} \)-limit of a sequence of \( \bar{d} \)-continuous channels is \( \bar{d} \)-continuous.

Proof: See [19].

IV. CHANNELS IN DIFFUSION-BASED MOLECULAR COMMUNICATION

This is the main section of our paper. In this section, we first state the general properties of diffusion-based molecular channel in Section IV.A. The abstract diffusion-based molecular channel model is given in Section IV.B and capacity theorems and channel coding theorems are proven in Section IV.C. Section IV.D discusses the implications and assumptions of our results.

A. General Descriptions

The theory of molecular communication studies the process of “transmission and reception of information encoded in molecules” [1]. In other words, in a molecular communication system, we utilize features of certain molecules as the information carrier, transmit the molecules through the communication media, and design a receiver which is capable of recognizing the features encoded over. The diffusion-based systems refer to those systems whose communication media are described by the “diffusion processes”. In the following we introduce the essential components of diffusion-based molecular communication systems:

1) Transmitter: In molecular communication, the transmitter has many choices of information carrier. For example, we can embed the information in the molecule concentration magnitudes [6], the inter-transmission times [8], the relative transmission times [20], the molecule types [21], or hybrids of each other [7], [8]. After the messages are encoded, the transmitter conveys the messages by simply releasing the encoded molecules into the communication media.

2) Communication Media: On contrast to the variety of information carrier, to the present days the communication media of molecular communication are concentrated on the fluid media almost exclusively. The fluid media represent the environment where the communication takes places. A typical environment is the blood, where the communication process occurs at human vessels.

As is well-known, the motion of molecules in fluid media is described by the “diffusion process”. The molecular communication systems whose communication media are described by the diffusion process are collectively called the “free diffusion-based molecular systems” or simply “diffusion-based molecular systems”. For systems operating under the diffusion
process, there is a special type of randomness which distinguishes those systems from the classical communication: the disorder of message arrivals. Consider an one-dimensional molecular communication system with transmitter and receiver separated by some distance (Fig. 1). For each released molecule diffusing independently in the fluid medium, the time it takes to be detected by the receiver is a random variable. If we assume that the receiver perfectly detects every molecule at its first arrival at the location of the receiver, then the detection times of the transmitted messages are the first passage times of the corresponding molecules, which are random variables depending only on the fluid medium, the corresponding transmitted molecules, and the distance from transmitter to receiver. Denote the first passage time of the $i$th message by $X_i$. It is possible to see that $X_i \leq X_j$ with positive probability even if $i > j$, i.e., it can happen that the later transmitted message arrives earlier. More generally, if we release a set of molecules in sequence, then it can happen that the receiver receives these molecules in any order.

The disorder of message arrivals is inevitable in diffusion-based molecular communication. Rather unfortunately, the classical tools dealing with disorders of message arrivals are targeting at the link-layer disorders (e.g., [22]) and do not suit the case of diffusion-based disorder. Specifically, there are no existing mathematical tools describing the behavior of random ordering of arbitrary set of infinite random variables. To cope with it, we must develop useful channel model that describes the phenomena of the random ordering of first passage times, and by useful we mean the capability of applying the existing communication theory to the channel. The following is the strategy we take: we first find out the essential features of first passages times occurring in diffusion-based systems and define the notion of permutation channel induced by the random ordering of first passage times. Afterwards, we prove that the permutation channel is with ADIMA, and apply the channel coding theorems to such channel.

Despite the randomness described above, the first passage times in diffusion-based molecular systems do contain some regularities. The followings are the essential properties of first passage times in diffusion-based systems:

- We require that the $X_{i+1}$ is a delayed version of $X_i$; that is, there are two independent random variables $D \geq 0$ and $D' \geq 0$ having the same distribution, and a random variable $T_i > 0$ independent of $D$ and $D'$, such that

  $$X_i = D,$$

  $$X_{i+1} = D' + T_i.$$  

The above condition actually says that we are releasing the encoded molecules in sequence (see Fig. 2). The intuitive meaning is that $T_i$ is the inter-transmission time of the $i$th and $(i + 1)$th messages, and $D$ (or $D'$) is the first passage distribution of the $i$th message. If we release the $i$th message, wait for a time $T_i$, and release the $(i + 1)$th message, then
the time it takes for the $i$th and $(i+1)$th molecules to diffuse to the receiver is of the above form. Note that the above condition can be applied iteratively on $i$ to derive

$$X_1 = D,$$

$$X_{i+1} = D' + \sum_{t=1}^{i} T_i,$$

where $D$ and $D'$ are independent and have the same distribution, and all $T_i$’s are independent. Note also that the $X_i$’s are pairwise independent.

Let us give some examples. If the system is “synchronous” (which is the case in [6], [8], and [20]) then $T_i = T$ for a real number $T > 0$ and $X_{i+1} = X_1 + iT$. The work in [8] also considers an asynchronous communication scheme for which $T_i$’s are i.i.d. random variables.

- The second restriction we impose on the first passage times is a qualitative one: we shall require that the arrival order of each $X_i$ is “effected” “most exclusively” by the $X_j$’s for those whose indices are close (or, equivalently, $|j-i|$’s are small). The precise meaning of “effected” and “most exclusively” are made clear by the next section, where we need the notion of the permutation channel to state them properly.

Our second restriction aims at capturing the nature of the diffusion processes occurring in molecular communication. The common feature of these diffusion processes is that if the release times of two molecules are pairwise independent and have the same distribution, and all $T_i$’s are independent. Note also that the $X_i$’s are i.i.d. random variables.

Let us give a concrete example to support the belief. Consider the diffusion process governed by the Brownian motion with drift, which is adopted in most diffusion-based molecular communication systems (see, e.g., [8], [20], and [21]). The first passage time of a released molecule is given by

$$f_D(t) = \begin{cases} \frac{x}{\sqrt{4\pi\nu t}^\frac{1}{2}} \exp\left(-\frac{(ut-x)^2}{4\nu t}\right), & t \geq 0 \\ 0, & t < 0 \end{cases}$$

where $\nu$ is the diffusion coefficient, $x$ is the distance from the transmitter to the receiver, and $v$ is the drifting velocity.

Suppose the inter-transmission times $T_i$’s are supported on $[t_i, \infty)$ and $\epsilon = \inf_i t_i > 0$. Then, according to the first restriction, the probability of the $i$th released molecule advancing the first is

$$P(X_i \leq X_1) = P(D' + \sum_{k=1}^{i} T_k \leq D)$$

$$\leq P(D - D' \geq i\epsilon)$$

$$\leq P(D \geq i\epsilon)$$

$$\leq \int_{i\epsilon}^{\infty} f_D(u)du.$$
Similar reasonings apply to \( P(X_i \leq X_j) \) with all \( i, j \)'s. In particular, if \( \epsilon \geq 1 \), then by union bound

\[
P(X_j \leq X_i \text{ or } X_{j+1} \leq X_i \text{ or } \cdots) \leq \sum_{s=j}^{\infty} P(X_s \leq X_i) \\
\leq \sum_{s=j}^{\infty} e^{-s} \\
\leq e \times e^{-j} \\
\to 0 \text{ as } j \to \infty.
\]

That is, the probability of the event “any molecule released after the \( j \)th message advancing the \( i \)th released molecule is vanishing in \( j \)”. This strong and universal property of diffusion processes is the one we shall capitalize upon when formulating the mathematical structure of diffusion-based molecular channels.

3) **Receiver:** In molecular communication, the receivers are designed to match the information carrier chosen by the transmitter. For example, if the information are carried on the molecule types, then the receiver is some nanomachines capable of recognizing these types. If the transmitter emits different concentration levels of a compound, then the receiver is usually a nanomachines capable of recognizing these types. If the transmitter emits different concentration levels of a compound, then the receiver is usually a nanomachines capable of recognizing these types.

For an integer \( n \), denote the set of symmetric group of order \( n \) by \( S_n \); that is, \( S_n \) is the set of all bijections of integers \( \{1, 2, \cdots, n\} \) onto itself. An element \( s \in S_n \) is called a permutation and can be represented by the permutation matrix:

\[
s = \begin{pmatrix}
1 & 2 & 3 & \cdots & n \\
b_1 & b_2 & b_3 & \cdots & b_n
\end{pmatrix}
\]

where \( \{b_1, b_2, \cdots, b_n\} \) exhausts \( \{1, 2, \cdots, n\} \), indicating the position after the effect of \( s \); that is, \( b_i = s(i), \ i = 1, 2, \cdots, n \). We also consider the infinite permutation defined as any bijection of the set of all integers \( I = \{\cdots, -2, -1, 0, 1, 2 \cdots\} \) onto itself. The set of all infinite permutations are denoted by \( S_I \). Similar to \( S_n \), any \( s \in S_I \) has its permutation matrix representation:

\[
s = \begin{pmatrix}
\cdots & -1 & 0 & 1 & \cdots \\
\cdots & b_{-1} & b_0 & b_1 & \cdots
\end{pmatrix}
\]

for some doubly infinite sequence \( \{b_i\}_{i \in I} \) as the position indicators.

Let \( \gamma \) be any probability measure on \( S_I \) (with Borel field being all subsets of \( S_I \) in discrete topology). The effect of

\[
s(x) = (x'), \ x'_i = x_{s^{-1}(i)} \text{ or equivalently } x'_{b_i} = x_i, \ i \in I,
\]

and \( \gamma(s) \) is, of course, the probability of such index permutation.

Given a finite set of random variables \( X_1, X_2, \cdots, X_n \), let \( X_{(i)} \) denote the \( i \)th largest order statistic of \( X_1, X_2, \cdots, X_n \); that is, \( X_{(1)} \geq X_{(2)} \geq \cdots \geq X_{(n)} \). The order statistics of \( X_i \)'s induce a probability measure \( \gamma \) on \( S_n \) by considering the probability \( \gamma(s) \) of

\[
s = \begin{pmatrix}
1 & 2 & 3 & \cdots & n \\
b_1 & b_2 & b_3 & \cdots & b_n
\end{pmatrix}
\]

as \( P(X_1 = X_{(b_1)}, X_2 = X_{(b_2)}, \cdots, X_n = X_{(b_n)}) \). We shall say that \( \gamma \) is induced by the ordering of \( X_i \)'s. For the case of \( S_I \) the ordering of an infinite sequence of random variables is ambiguous. To this end, we need another way of identifying the bijections in \( S_I \). For a finite subindex set \( \{k_i\}_{i=1}^{n} \) (i.e., \( k_i \)'s are integers and \( k_1 < k_2 < \cdots < k_n \)) and a \( s \in S_I \),

\[
s = \begin{pmatrix}
\cdots & -1 & 0 & 1 & \cdots \\
\cdots & b_{-1} & b_0 & b_1 & \cdots
\end{pmatrix},
\]
define the local \( \{k_i\}_{i=1}^n \) version of \( s \) as
\[
\begin{pmatrix}
k_1 & k_2 & k_3 & \cdots & k_n \\
b'_1 & b'_2 & b'_3 & \cdots & b'_n
\end{pmatrix}
\]
where \( b'_i \) is the \( i \)th least integer of \( b_{k_1}, b_{k_2}, \cdots, b_{k_n} \). For example, the local \( \{1, 3, 5\} \) version of
\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 \\
5 & 4 & 3 & 1 & 2
\end{pmatrix}
\]
is
\[
\begin{pmatrix}
1 & 3 & 5 \\
3 & 2 & 1
\end{pmatrix}
\]
since \( 5 > 3 > 2 \). Obviously, for \( s, s' \in S_I \), \( s = s' \) if and only if every local version of \( s \) and \( s' \) coincides. Therefore, if we view the local \( \{k_i\}_{i=1}^n \) version as the permutation matrix induced by the order statistics on the random variables \( X_{k_1}, X_{k_2}, \cdots, X_{k_n} \), then these partial orderings of the infinite sequence \( \{\cdots, X_{-1}, X_0, X_1, \cdots\} \) uniquely determine an infinite permutation \( s \in S_I \). However, the explicit close-form solution of the distribution \( \gamma \) on \( S_I \) induced by \( \{\cdots, X_{-1}, X_0, X_1, \cdots\} \) is a difficult and long standing problem for which all existing solutions require strong assumptions (see, e.g., the case for i.i.d. and exchangeable random variables in [23]). Fortunately, we can take a different route to consider the qualitative properties of \( \gamma \) and the qualitative features are enough for our application, as illustrated below.

We shall say that a probability measure \( \gamma \) on \( S_I \) is induced by the orderings of \( \{\cdots, X_{-1}, X_0, X_1, \cdots\} \) if \( \gamma \) possesses the following property: for any finite subindex \( \{k_i\}_{i=1}^n \) and any set of integers \( b'_1, b'_2, \cdots, b'_n \) exhausting \( \{1, 2, \cdots, n\} \), we have
\[
P(X_{k_1} = X_{(b'_1)}, \cdots, X_{k_n} = X_{(b'_n)}) = \sum \gamma(s)
\]
where the summation is taken over all \( s \in S_I \) with local \( \{k_i\}_{i=1}^n \) version
\[
\begin{pmatrix}
k_1 & k_2 & k_3 & \cdots & k_n \\
b'_1 & b'_2 & b'_3 & \cdots & b'_n
\end{pmatrix}
\]
In other words, for any finite sub-collection \( \{X_{k_1}, \cdots, X_{k_n}\} \) of \( \{\cdots, X_{-1}, X_0, X_1, \cdots\} \), we demand that the probability of the event \( \{X_{k_1} = X_{(b'_1)}, \cdots, X_{k_n} = X_{(b'_n)}\} \) equals the sum of probability of the infinite permutations for which their local \( \{k_i\}_{i=1}^n \) versions are the permutation matrix generated by the ordering of \( \{X_{k_1}, \cdots, X_{k_n}\} \).

For difficulty illustrated before, the explicit construction for \( \gamma \) satisfying the condition (2) is beyond the scope of this paper. In particular, the uniqueness of \( \gamma \) is not of our concern: any \( \gamma \) with property (2) is a good model for the channel under our consideration. If \( \gamma \) is not unique we can simply choose any one as the representative.

We are now ready to define the notion of a permutation channel. Let \( x = (\cdots, x_{-1}, x_0, x_1, \cdots) \) be any input sequence of a diffusion-based molecular communication system. As discussed in Section IV.A.2, \( x \) corresponds a set of random variables \( \{X_i\}_{i \in I} \) where \( X_i \) is the first passage time of the message \( x_i \). The ordering of these first passage times then induces a probability measure \( \gamma_x \) on \( S_I \). The permutation channel \( \{\nu_x\}_x \) on a same input and output alphabet, say \( A \), is defined by
\[
\nu_x(y) = \gamma_x(s), \quad y = s(x), \quad x, y \in A_{\infty},
\]
where \( s \in S_I \) and \( y = s(x) \) means (1). With slight abuse of notation we also say that \( \{\gamma_x\}_x \) or \( \gamma \) is a permutation channel.

With the help of the permutation channel, we now give the following characterizations of a new class of channel, which is the mathematical channel model capturing all essential features of diffusion-based molecular channels considered in Section IV.A.

**Definition 1** (The Diffusion-Based Molecular Channel). A diffusion-based molecular channel \( [A, \nu, B] \) is a cascade of a permutation channel \( \gamma \) on \( A \) and a stationary ergodic ADIMA channel \( [A, \eta, B] \), where \( \gamma \) is induced by the first passage times of input messages. \( [A, \eta, B] \) is called the receiver channel. The permutation channel has the following property: Let \( x \) and \( x' \) be two input sequences and induce \( \gamma_x \) and \( \gamma_{x'} \) on \( S_I \), respectively. For \( \epsilon > 0 \), there exists integers \( m \) and \( m' \) with \( m' \leq m \) such that for all integer \( n \), if \( x_i = x'_i \) for \( -m \leq i \leq n + m \), then the following holds:

![Fig. 3: Diffusion-Based Molecular Channel](image-url)
For any \( s \in S_I \) with \( \sup_{i=0,1,\ldots,n} s^{-1}(i) \leq m' + n \) and \( \inf_{i=0,1,\ldots,n} s^{-1}(i) \geq -m' \), we have \(|\gamma_x(s) - \gamma_{x'}(s)| < \epsilon\).

The "outlier" probability is small:

\[
P( \sup_{i=0,1,\ldots,n} s^{-1}(i) > m' + n \text{ or } \inf_{i=0,1,\ldots,n} s^{-1}(i) < -m' ) < \epsilon
\]

in both \( \gamma_x \) and \( \gamma_{x'} \) measure. In other words,

\[
\sum_s \gamma_x(s) < \epsilon, \quad \sum_s \gamma_{x'}(s) < \epsilon
\]

where the summation is taken over all \( s \) with the property in the probability bracket.

Let us give the engineering interpretation to all the assumptions we made. In section IV.A we have illustrated that the messages arrive at the receiver in disorder for diffusion-based molecular communication systems. Since such disorder comes from the random ordering of the first passage times, it does contain some implicit regularities. Suppose we aim at an interval such that the "crossing probability \( P(X_j \leq X_i) \)" is small in \( j - i \), which is the content of condition (ii).

The total effect at the receiver is simply modeled as an ADIMA channel. The notion of ADIMA already characterizes fairly well a receiver whose detection of a message is "mostly" effected by its nearby received messages.

C. Channel Capacity

In this section we shall prove the following fundamental theorem of diffusion-based molecular communication:

**Theorem 6** (The Fundamental Theorem of Diffusion-Based Molecular Communication). Let \( A \) be a finite alphabet. For a diffusion-based molecular channel \([A,\nu,B]\) with a stationary ergodic source \([A,\mu]\),

a) \( C = C_e = C_s = C^* = C_{eb} = C_{seb} \).

b) If \( R < C \) and \( \epsilon > 0 \), then for sufficiently large \( n_0 \) there exist \( < 2^{nR} >, n, \epsilon \) block codes for all \( n \geq n_0 \). If \( R > C \) there exists an \( \epsilon_{\min} > 0 \) such that there do not exist \( < 2^{nR} >, n, \epsilon \) block codes for any \( \epsilon < \epsilon_{\min} \).

c) If \( H(\mu) < C \), then \( \mu \) is admissible. If \( H(\mu) > C \), then \( \mu \) is not admissible.

We divide our proof into the following steps:

(i) The permutation channel in a diffusion-based molecular channel is stationary.

(ii) The permutation channel in a diffusion-based molecular channel is with ADIMA.

(iii) The cascade of ADIMA channels is an ADIMA channel.

(iv) By **Theorem 3**, an ADIMA channel is \( d \)-continuous, and therefore **Theorem 4.a)~d)** apply.

(v) The diffusion-based molecular channel is strongly mixing (and therefore by **Theorem 2** it is ergodic).

(vi) The cascade of two ergodic channels is ergodic. By **Theorem 4.e)** the proof is complete.

**Proof**: (i): This is an immediate result of the fact that \( Ty = s(Tx) \) if and only if \( y = s(x) \), where \( T \) is the time-shift operator.

(ii): Since by (i) the channel is stationary, it suffices to prove that for any \( \epsilon > 0 \) and all integer \( n \), there exists an integer \( m = m(\epsilon) \) such that if \( x_i = x'_i \) for \(-m \leq i \leq n + m\), then \( |\nu^n_x(F) - \nu^n_{x'}(F)| < \epsilon \) for any \( F \in B_\Lambda(0,n) \). Let \( \epsilon > 0 \) and \( F \) be given. Let \( m \) be a large integer determined later and \( x_i = x'_i \) for \(-m \leq i \leq n + m\). For each integer \( m' \), divide the elements of \( y^n_0 \in F \) into three classes \( F_{1m}', F_{2m}' \), and \( F_2m' \) where

\[
F_{1m}' = \{ y^n_0 \mid \exists s \in S_I \text{ with } \sup_{i=0,1,\ldots,n} s^{-1}(i) \leq m' + n \text{ and } \inf_{i=0,1,\ldots,n} s^{-1}(i) \geq -m' \text{ such that } (s(x))^n_0 = y^n_0 \},
\]
\[ F_1^{m'} = \{ y_0^n | \exists s \in S_f \text{ with } \sup_{i=0,1,\ldots,n} s^{-1}(i) \leq m' + n \] and \[ \inf_{i=0,1,\ldots,n} s^{-1}(i) \geq -m' \text{ such that } (s(x'))_0^n = y_0^n \}, \]

and \( F_2^{m'} \) is the complement of \( F_1^{m'} \cup F_1^{m'}. \) If \( m' < m, \) then \( x_i = x_i' \) for \( m' \leq i \leq m + n \) and therefore \( F_1^{m'} \) actually equals \( F_2^{m'} \). Now, by definition of a diffusion-based molecular channel, there is an \( m \) such that if \( y_0^n \in F_1^{m'} \), then

\[ |\gamma^n_x(y_0^n) - \gamma^n_{x'}(y_0^n)| < \epsilon \]

since there exists a \( s \in S_f \) with \( \sup_{i=0,1,\ldots,n} s^{-1}(i) \leq m' + n \) and \( \inf_{i=0,1,\ldots,n} s(i) \geq -m' \) such that \( (s(x))_0^n = (s(x'))_0^n. \)

On the other hand, if \( y_0^n \in F_2^{m'}, \) then either \( \sup_{i=0,1,\ldots,n} s^{-1}(i) > m' + n \) or \( \inf_{i=0,1,\ldots,n} s^{-1}(i) < -m'. \) By definition of the diffusion-based molecular channel,

\[ |\gamma^n_x(y_0^n) - \gamma^n_{x'}(y_0^n)| \leq |\gamma^n_x(y_0^n)| + |\gamma^n_{x'}(y_0^n)| \leq 2\epsilon. \]

Since any set \( F \in B_A(0, n) \) is a finite union of \( y_0^n, \) the proof is complete.

(iii): We shall state the result formally and prove it in appendix A.

(iv): It is a fact.

(v): Let \( C_1 = C(y_0^n) \) and \( C_2 = C(y_0^n) \) be two cylinder sets. The time indices 0, \( n, \ p, \) and \( q \) are chosen for convenience and can be replaced by any other time. Without loss of generality suppose that \( n - 0 \geq q - p. \) Since \( T^k C(y_0^n) = C(y_0^n) C(y_0^n + k), \)

\[ P(C_1 \cap T^k C_2 | x) = P(C(y_0^n) \cap C(y_0^n + k) | x) \]

\[ = \gamma_x(\{ s | s(x) \in (y_0^n) \cap (y_0^n + k) \}) \]

\[ = \gamma_x(C(y_0^n) \cap C(y_0^n + k) | s \in S_1^n)P(s \in S_1^n) \]

\[ + \gamma_x(C(y_0^n) \cap C(y_0^n + k) | s \in S_2^n)P(s \in S_2^n) \]

where \( C(y_0^n) \cap C(y_0^n + k) \) means (of course) \( \{ s | s(x) \in (y_0^n) \cap (y_0^n + k) \}, \)

\[ S_1^n = \{ s | \sup_{i=0,1,\ldots,n} s(i) \leq m + n \text{ and } \inf_{i=0,1,\ldots,n} s(i) \geq -m \}, \]

\[ S_2^n = (S_1^n)^c. \]

By the definition of a diffusion-based molecular communication channel, there is a large \( m \) such that \( P(S_2^n) < \epsilon \) and therefore

\[ P(S_2^n) = 1 - P(S_2^n) > 1 - \epsilon. \]

Now, choose \( k > 2m + n + p \) so that the intervals \((-m, -m + 1, \ldots, m + n)\) and \((-m + p + k, -m + p + k + 1, \ldots, m + q + k)\) are disjoint. Since

\[ s(x) \in C(y_0^n) \iff (s(x))_0^n = y_0^n, \]

for \( s \in S_1^n \) this implies that \( s(x) \in C(y_0^n) \) if and only if \( y_0 = x_0, y_1 = x_1, \ldots, y_n = x_n, \) \( -m \leq x_0, x_1, \ldots, x_n \leq m + n \). By (2), the measure of the union of such \( s' \) is the probability of the event \( \{ X_0 = X_{i_0'}, X_1 = X_{i_1'}, \ldots, X_n = X_{i_n'} \} \) where the local \( \{ 0, 1, \ldots, n \} \) version of \( s \) is

\[ \left( \begin{array}{cccc} 0 & 1 & 2 & \cdots & n \\ i_0' & i_1' & i_2' & \cdots & i_n' \end{array} \right). \]

In other words,

\[ \gamma_x(C(y_0^n) | S_1^n) = P(\cup_{i_0', \ldots, i_n'} \{ X_0 = X_{i_0'}, \ldots, X_n = X_{i_n'} \}) \]

where \( 0 \leq i_0', \ldots, i_n' \leq n \) and \( \{ i_0', \ldots, i_n' \} \) exhausts \( \{ 0, 1, \ldots, n \}. \) Likewise, since the channel is stationary, for \( s \in S_1^n \) we have \( s(x) \in C(y_0^n) \) if and only if \( y_{p+k} = x_{i_{p+k}}, y_{p+k+1} = x_{i_{p+k+1}}, \ldots, y_{q+k} = x_{i_{q+k}}, -m + p + k \leq i_{p+k}, \ldots, i_{q+k} \leq m + k + q, \) and

\[ \gamma_x(C(y_0^n) | S_1^n) = \]

\[ \gamma_x(C(y_0^n) | S_1^n) = \]

\[ P(\cup_{i_0', \ldots, i_{q-k}} \{ X_0 = X_{i_0'}, \ldots, X_{q+k} = X_{i_{q-k}} \}). \]
Since the index sets of \( \{X_i\}_{i=1}^n \) and \( \{X_j\}_{j=p+k}^{q+k} \) are disjoint and all \( X_i \)'s are pairwise independent, we have, for large \( k \),

\[
\gamma_x(C(y^n_0) \cap C(y^{q+k}_p)|S^m_2) = \gamma_x(C(y^{q+k}_p)\cap C(y^n_0)|S^m_2)
\]

and

\[
|P(C_1 \cap T^k C_2|S^m_2)P(S^m_2) - P(C_1|S^m_2)P(S^m_2)P(T^k C_2|S^m_2)P(S^m_2)| \leq 2\epsilon.
\]

Combining the above results shows that the permutation channel in a diffusion-based molecular channel is strongly mixing. By Theorem 2, it is also ergodic.

(vi): By examining the definition of ergodicity of a channel, we see that, since the source together with the permutation channel can be viewed as another source to the receiver channel (which by definition is ergodic), the overall channel is ergodic. The above reasoning carries over to cascade of arbitrary number of ergodic channels.

\[\Box\]

D. Remarks on Theorem 6

The Theorem 6 provides the mathematical foundations for information theory in diffusion-based molecular communication. In this section, we discuss several issues concerning the assumptions of the Theorem 6 along with some important implications.

- Byproducts of Theorem 6

The proof of Theorem 6 contains many useful byproducts. We list them formally as below:

**Theorem 7** (Stationarity of a Diffusion-Based Molecular Channel). A diffusion-based molecular channel is stationary.

**Proof:** This is an easy consequence of the fact that the permutation channel and the receiver channel are both stationary, and the cascade of two stationary channels are stationary.

**Theorem 8** (The Permutation Channel). The permutation channel in a diffusion-based molecular channel is with ADIMA, strongly \( \bar{d} \)-continuous, and \( \bar{d} \)-continuous.

**Theorem 9** (Ergodicity of the Diffusion-Based Molecular Channel). A diffusion-based molecular channel is ergodic.

**Theorem 10** (\( \bar{d} \)-Continuity of the Diffusion-Based Molecular Channel). A diffusion-based molecular channel is \( \bar{d} \)-continuous.

- Why \( \bar{d} \)-Continuity?

In the proof of Theorem 6 we have shown that the diffusion-based molecular channel is an ADIMA channel. Since ADIMA channel has its own coding theorems, it seems better to directly view the diffusion-based molecular channel as ADIMA channel and not bothering using the \( \bar{d} \)-continuity. This is, however, not appropriate due to the fact that the ADIMA channel is very “vulnerable” to modeling errors. This is best illustrated by the following example. Consider two i.i.d. binary sources with parameter \( p \) and \( q \). Recall that an ADIMA channel demands the variational distances between distributions under consideration to be close, which is not the case for these two i.i.d. sources when \( p \neq q \) since the variational distance \( v_n \) between the two i.i.d. sources tends to 1 as \( n \rightarrow \infty \), no matter how small the error \( |p - q| > 0 \) is. The example tells us that if our model differs slightly from the reality, then the theorem might not carry over. Unfortunately, the diffusion process is itself a mathematical assumption and not the physical reality. In particular, for the most widely adopted diffusion model, the Brownian motion, various peculiar physical behaviors have been reported (e.g., almost-surely nowhere-differentiable path) and now it is commonly accepted that the Brownian motion is a good approximation of diffusion process but not the exact solution. There do exist realistic models for diffusion processes (e.g., the Ornstein-Uhlenbeck process), but they usually involve the “stochastic differential equations” which render the derivation of analytical results hard, if not impossible.

On contrast to the ADIMA channel, the \( \bar{d} \)-continuity is very “robust” to the modeling errors [20]. In particular, by Theorem 5 the \( \bar{d} \)-limit of a sequence of \( \bar{d} \)-continuous channels is \( \bar{d} \)-continuous, while the limit of a sequence of ADIMA channels is not necessarily an ADIMA channel. This tells us that suppose we can approximate the “true” channel by a sequence of \( \bar{d} \)-continuous channels, then the results we derived are still valid for the “true” channel. This is the reason we adopt the \( \bar{d} \)-continuity in this work.
Continuous alphabets are possible. In molecular communication, it can happen that the input and output alphabets are continuous (a classical example being the transmission of concentration waveforms over fluid media). We point out that there do exist works on the \(d\)-continuous channel with continuous input and output alphabets. The extension of our results to continuous alphabets is therefore possible.

Why ergodic sources?
The notion of ergodicity comes from the statistical physics, where the introduce of ergodic process is used to describe a closed physical system. Since a large application area of molecular communication is to monitor the physical systems occurring in biological world, we are naturally lead to consider the ergodic sources. Besides, in most cases of communication a transmitter is itself a closed physical system, thus justifying the use of ergodicity. Last but not least, the ergodic sources have so many strong mathematical properties that we could barely derive anything without it. We just can’t help but using it (and so do many great predecessors in information theory).

Why \(C_{cb}\), \(C^*\), and \(C_{scb}\)?
\(C_{cb}\) clearly has its importance in coding theory. The importance of \(C_{scb}\) and \(C^*\) is not so obvious, as we illustrated below. A major application of molecular communication is the monitoring of biological processes (e.g., the output signal of a human organ), which is usually assumed to be ergodic. For such scenarios, our communication problem at hand is “Given an ergodic source \([A, \mu]\) and a diffusion-based molecular channel \([A, \nu, B]\), what is the best we can do?” The question is answered in a very strong sense by the definition of \(C_{scb}\) and Theorem 6: a good source/channel code for \([A, \mu]\) exists if \(H(\mu) < C_{scb}\); if \(H(\mu) > C_{scb}\), no good source/channel code exist.

The reason for taking \(C^*\) into consideration is of practical concern. Suppose that we try to really find out the channel capacity of the permutation channel \(\gamma\). To this end, the direct calculation of \(H(\mu), H(\mu+\gamma)\), and \(H(\mu+\gamma)\) involves all combinatorial terms for each \(N\) (i.e., for each \(N\) and a realization \((x_1, x_2, \ldots, x_N)\) and \((y_1, y_2, \ldots, y_N)\), we must consider all \(s \in S_t\) for which \(s(x) = y\) and the passing of limit \(N \to \infty\). On contrast, since \(C^*\) is defined through the sample mutual information \(i_n(x^n, y^n)\), it suffices to choose a large \(N\), calculate the expectation of \(i_N(x^n, y^n)\), and the convergence of \(i_n(x^n, y^n)\) in \(L_1\) and the Shannon-McMillan Theorem will guarantee the closeness of \(i_N(x^n, y^n)\) and \(I(\mu)\).

V. Conclusions
As a promising paradigm for nano-communication, the molecular communication has been developed over the past decade. In this paper, we consider a major subclass of molecular communication systems called the diffusion-based molecular systems. Solid mathematical foundations for information theory are laid down for diffusion-based molecular communication. In particular, we have created an abstract channel model capturing all the essential features of diffusion-based molecular systems, and for such channel, the capacity theorems and channel coding theorems are proven. Other useful notions concerning stationarity and ergodicity of diffusion-based molecular channel are also established.

APPENDIX A
CASCADE OF ADIMA CHANNELS
Although the generalization is possible, here we shall confine ourselves to a special case which suffices our purpose.

Theorem 11 (Cascade of ADIMA Channels). For channels with finite input and output alphabets, the cascade of ADIMA channels is an ADIMA channel.

Proof: It suffices to consider the cascade of two ADIMA channels. The case for cascade of arbitrary number follows from induction. Let \([A, \sigma, Q]\) and \([Q, \eta, B]\) be two ADIMA channels with finite input and output alphabets and let \([A, \nu, B]\) be their cascade. Fix \(\epsilon > 0\). Since \(\eta\) is with ADIMA, for any \(n\) there are integers \(m'\) and \(a'\) such that for any \(y \in B_0^n\),
\[
|\eta_z(y) - \eta_{z'}(y)| \leq \epsilon
\]
if \(z_i = z_i'\) for \(-m' \leq i \leq n + a'\). Write
\[
\nu_z(y) = \int_{Q_{m'}^\infty} \eta_u(y) d\sigma_z(u)
= \sum_{z \in Q_{a'n}^{m' - n}} \int_{C(z)} \eta_u(y) d\sigma_z(u).
\]
By (3), we have
\[
\sup_{u, w \in C(z)} |\eta_u(y) - \eta_w(y)| \leq \epsilon.
\]
Put $\eta_{C(z)}(y) = \inf_{u \in C(z)} \eta_u(y)$. Then we can further write

$$\sum_{z \in Q^{a+n}_{-m'}} \sigma_x(C(z)) \eta_{C(z)}(y) \leq \nu_x(y) \leq \sum_{z \in Q^{a+n}_{-m'}} \sigma_x(C(z))(\eta_{C(z)}(y) + \epsilon).$$

Therefore,

$$|\nu_x(y) - \nu_{x'}(y)| \leq \sum_{z \in Q^{a+n}_{-m'}} |\sigma_x(C(z)) - \sigma_{x'}(C(z))| \times \text{Constant} \leq |Q^{a+n}_{-m'}| \times \text{Constant} \times \epsilon$$

if $x$ and $x'$ are chosen with integers $m$ and $a$ such that $x_i = x'_i$ for $m \leq i \leq n + a$ implies $|\sigma_x(C(z)) - \sigma_{x'}(C(z))|$ is small, where the condition can be achieved since $[A, \sigma, Q]$ is with ADIMA. The proof is completed by noting that all $F \in B_B(0, n)$ is a finite union of $y \in B^n_0$.

ACKNOWLEDGMENT

The authors would like to thank Prof. Ian F. Akyildiz for his inspiring advice during a meeting in Taiwan. The authors would also like to thank Prof. Kwang-Cheng Chen, Prof. Chia-Han Lee, Po-Jen Shih, and Yen-Chi Lee for their contribution to this paper.

REFERENCES

[1] I. F. Akyildiz, J. M. Jornet, and M. Pierobon, “Nanoworks: a new frontier in communications,” Communications of the ACM, vol. 54, no. 11, pp. 84–89, 2011.
[2] D. L. Nelson and M. M. Cox, Lehninger Principles of Biochemistry, Fourth Edition, fourth edition ed. W. H. Freeman. Apr. 2004.
[3] W. H. Bossert and E. O. Wilson, “The analysis of olfactory communication among animals,” Journal of Theoretical Biology, vol. 5, no. 3, pp. 443 – 464, 1967.
[4] L. Parcerisa Giné and I. F. Akyildiz, “Molecular communication options for long range nanonetworks,” Comput. Netw., vol. 53, no. 16, pp. 2753–2766, Nov. 2009.
[5] T. Nakano, T. Sada, M. Moore, R. Egashira, A. Enomoto, and K. Arima, “Molecular communication for nanomachines using intercellular calcium signaling,” in IEEE NANO 2005, 2005.
[6] L.-S. Meng, P.-C. Yeh, K.-C. Chen, and I. Akyildiz, “A diffusion-based binary digital communication system,” in Communications (ICC), 2012 IEEE International Conference on, June 2012, pp. 4985 –4989.
[7] Y.-P. Hsieh, Y.-C. Lee, P.-J. Shih, P.-C. Yeh, and K.-C. Chen, “On the asynchronous information embedding for event-driven systems in molecular communications,” Nano Communication Networks, no. 0, pp. --, 2012.
[8] Y.-P. Hsieh, P.-J. Shih, Y.-C. Lee, P.-C. Yeh, and K.-C. Chen, “An asynchronous communication scheme for molecular communication,” in Communications (ICC), 2012 IEEE International Conference on, June 2012, pp. 6177 –6182.
[9] A. Einolghozati, M. Sardari, A. Beirami, and F. Fekri, “Capacity of discrete molecular diffusion channels,” in Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on, 31 2011-aug. 5 2011, pp. 723 –727.
[10] M. Pierobon and I. Akyildiz, “Information capacity of diffusion-based molecular communication in nanonetworks,” in INFOCOM, 2011 Proceedings IEEE, April 2011, pp. 506 –510.
[11] ——, “Capacity of a diffusion-based molecular communication system with channel memory and molecular noise,” Information Theory, IEEE Transactions on, vol. 59, no. 2, pp. 942 –954, Feb. 2013.
[12] C. E. Shannon, “A mathematical theory of communication,” The Bell System Technical Journal, vol. 27, pp. 379–423, 623–, July, October 1948.
[13] B. Mcmillan, “The Basic Theorems of Information Theory,” Ann. Math. Stat., vol. 24, pp. 196–219, 1953.
[14] A. Feinstein, “A new basic theorem of information theory,” 1954.
[15] A. Khinchin, Mathematical foundations of information theory, ser. Dover books on advanced mathematics. Dover Publications, 1957.
[16] E. Paffelhuber, “Channels with asymptotically decreasing memory and anticipation,” Information Theory, IEEE Transactions on, vol. 17, no. 4, pp. 379 – 385, Jul. 1971.
[17] R. Gray and D. Ornstein, “Block coding for discrete stationary -continuous noisy channels,” Information Theory, IEEE Transactions on, vol. 25, no. 3, pp. 292 – 306, may 1979.
[18] S. Verdu and T. S. Han, “A general formula for channel capacity,” Information Theory, IEEE Transactions on, vol. 40, pp. 1147–1157, 1994.
[19] D. Neuhoff and P. Shields, “Channels with almost finite memory,” Information Theory, IEEE Transactions on, vol. 25, no. 4, pp. 440 – 447, jul 1979.
[20] A. Eckford, “Nonascale communication with brownian motion,” Information Sciences and Systems CISS 07 41st Annual Conference on, p. 6, 2007.
[21] ——, “Achievable information rates for molecular communication with distinct molecules,” in Bio-Inspired Models of Network, Information and Computing Systems, 2007. BioNets 2007. 2nd, dec. 2007, pp. 313 –315.
[22] J. Walsh and S. Weber, “Capacity region of the permutation channel,” in Communication, Control, and Computing, 2008 46th Annual Allerton Conference on, 2008, pp. 646–652.
[23] S. Karlin and H. M. Taylor, A First Course in Stochastic Processes, Second Edition, 2nd ed. Academic Press, Apr. 1975.
[24] B. Atakan and O. B. Akan, “An information theoretical approach for molecular communication,” in 2007 2nd Bio-Inspired Models of Network, Information and Computing Systems. IEEE, 2007, pp. 33–40.
[25] J. Pittman, Combinatorial stochastic processes, ser. Lecture Notes in Mathematics. Berlin: Springer-Verlag, 2006, vol. 1875.
[26] R. M. Gray, D. L. Neuhoff, and P. C. Shields, “A generalization of the orinstein’s distance with application to information theory,” Annals of Probability, vol. 3, Apr. 1975.
[27] Y. Kadota, “On the capacity of asymptotically memoryless continuous-time channels (corresp.),” IEEE Trans. Inf. Theor., vol. 19, no. 4, pp. 556–557, Sep. 2006.
[28] I. F. Akyildiz and J. M. Jornet, “The internet of nano-things,” Wireless Commun., vol. 17, pp. 58–63, 2010.
