Multiple Access Analog Fountain Codes

Mahyar Shirvanimoghaddam, Yonghui Li and Branka Vucetic
School of Electrical and Information Engineering, The University of Sydney, NSW, Australia
Emails:{mahyar.shirvanimoghaddam, yonghui.li, branka.vucetic}@sydney.edu.au

Abstract—In this paper, we propose a novel rateless multiple access scheme based on the recently proposed capacity-approaching analog fountain code (AFC). We show that the multiple access process will create an equivalent analog fountain code, referred to as the multiple access analog fountain code (MA-AFC), at the destination. Thus, the standard belief propagation (BP) decoder can be effectively used to jointly decode all the users. We further analyze the asymptotic performance of the BP decoder by using a density evolution approach and show that the average log-likelihood ratio (LLR) of each user’s information symbol is proportional to its transmit signal to noise ratio (SNR), when all the users utilize the same AFC code. Simulation results show that the proposed scheme can approach the sum-rate capacity of the Gaussian multiple access channel in a wide range of signal to noise ratios.

Index Terms—Analog fountain codes, belief propagation, multiple access channel.

I. INTRODUCTION

Multiple access technologies, enabling multiple users to share common radio resources to fulfill their own transmission requirements, have been widely studied over decades. Successive decoding has been proved to be efficiently used to approach the corner points of the well known capacity region of the multiple access channel (MAC), while the middle part is achieved by additional rate splitting or time sharing [1]. Moreover, multiuser communication techniques such as code-division multiple access (CDMA), that allow for more robust and less complex joint detection/decoding, have had limited success in achieving the inner points of the MAC capacity region. The problem will be more challenging when all the users transmit with the same rate and power, as there is no structural irregularity to initiate the decoding convergence due to the fact that all the users are operating under the same conditions.

Recently, rateless codes have been applied in the multiple access scenario, where different users use them to adapt to the time varying wireless channel. In existing rateless multiple access (RMA) schemes [2][3][4], each user encodes its packets using a separate rateless code. Thanks to the rate adaptation property of rateless codes, without knowledge of channel state information (CSI) or frequent feedback information from the destination, RMA achieves an excellent performance on multiuser detection over both erasure and noisy channels. However, RMA conducts separate decoding for each user at the destination and soft decoding information is exchanged between several decoders in each iteration of the decoding algorithm; thus, not practical for systems with a large number of users.

Spatial coupling effects have been recently explored to increase the transmission efficiency in multiple access channels [5][6][7]. In [8], spatial coupling was applied to the erasure random access channel and the iterative interference cancelation process has been modeled as the erasure recovery process of low-density parity-check (LDPC) codes over a binary erasure channel (BEC). Although this approach can achieve a high throughput over erasure MACs, it cannot be used in wireless channels, where the collided packets are affected by fading and noise. To overcome this problem, authors in [1] showed that the capacity of a Gaussian MAC can be achieved by using a spatially coupled sparse graph multi-user modulation with an iterative interference cancelation scheme at the receiver. However, this approach performs decoding and interference cancelation separately and its complexity increases significantly as the number of active users increases.

In this paper, we propose a novel multiple access scheme based on a newly proposed capacity approaching analog fountain code (AFC) [9] to approach the sum-rate capacity of the multiple access. In the proposed scheme, referred to as multiple access analog fountain code (MA-AFC), each user uses an AFC code to generate a potentially limitless number of coded symbols. As the sum of coded symbols from various users is received at the destination, the received signals at the destination can be seen as coded symbols of an equivalent AFC code with a larger code degree. As a result, the standard belief propagation (BP) decoder can be used to jointly decode all the users at the destination. We analyze the decoding performance through density evolution analysis and show that the average LLR of each user is proportional to its transmit SNR. Simulation results show that the proposed scheme can approach the sum-rate capacity of the Gaussian multiple access channel in a wide range of SNRs and can be effectively applied to systems with a large number of users due to the linear complexity of the encoding and decoding of AFCs. Throughout the paper, we use boldface letters to denote the vectors, where the $i^{th}$ entry of vector $v$ is denoted by $v_i$. Matrices are represented by boldface capital letters, $G$, where $g_{i,j}$ is the $j^{th}$ entry in the $i^{th}$ row of $G$ and $G'$ is the transpose of $G$.

The rest of the paper is organized as follows. In Section II, we present the system model. The proposed multiple access scheme is presented in Section III. Section IV presents the decoding algorithm and the asymptotic analysis of the belief propagation decoding of the MA-AFC scheme based on the density evolution analysis. Simulation results are shown in Section V, and finally conclusions are drawn in Section VI.
We consider a communication system consisting of $M$ users, $U_1, U_2, ..., U_M$, out of which a subset $\mathcal{S} \neq \emptyset$ is active. That is only the users in the set $\mathcal{S}$ are transmitting to a common destination, $D$, as shown in Fig. 1. Each active user has $k$ binary information symbols to be delivered at the destination. The transmission model is time slotted, where at each time slot $i \geq 1$, an active user $U_j$ transmits a rateless coded symbol $u_{i,j}$ to the destination. The received signal $y_i$ at the destination at time instant $i$ is given by:

$$y_i = \sum_{j \in \mathcal{S}} h_{i,j} u_{i,j} + n_i,$$

where $h_{i,j}$ denotes the channel coefficient for $U_j$ and $\{n_i\}_{i=1}^{\infty}$ is a sequence of i.i.d. Gaussian random variables with zero mean and unit variance. The set of active users, $\mathcal{S}$, is known to the receiver; however, the transmitters only know whether they belong to $\mathcal{S}$ or not.

From an information theoretic point of view, for a $M$-user Gaussian MAC where there are $M$ users with power constraints ($P_1, P_2, ..., P_M$) and unit variance AWGN noise with zero mean, any rate $R_i$ can be achieved by $U_i$ as follows:

$$R_S \triangleq \sum_{i \in \mathcal{S}} R_i < \frac{1}{2} \log_2(1 + \sum_{i \in \mathcal{S}} P_i),$$

where $R_S$ is defined as the sum-rate of active users. Moreover, the upper bound can be achieved when the output signal distribution of each active user follows the Gaussian distribution $\mathcal{N}(0, P_i)$ [10].

### III. MULTIPLE ACCESS ANALOG FOUNTAIN CODES

Analog fountain codes (AFC) have been recently proposed in [9] as an effective rateless transmission scheme to approach the capacity of wireless channels. AFC is rateless in nature as a potentially limitless number of coded symbols can be generated, which enables the transmitter to effectively adapt to unknown channel conditions. In this section, we first briefly introduce the AFC code and then a general extension of AFC codes, denoted by multiple access analog fountain code (MA-AFC), is proposed.

#### A. Analog Fountain Codes

In AFC, the entire message of length $k$ binary symbols is first BPSK modulated to obtain a vector of modulated information symbols, $b_{1 \times k}$. To generate each coded symbol, $u_i$, first an integer $d$, called degree, is obtained based on a predefined probability distribution function, called degree distribution, for $i = 1, 2, ..., n$. Then, $d$ randomly selected modulated information symbols are linearly combined with real weight coefficients to generate one coded symbol. For simplicity, we assume that the degree of each coded symbol is fixed, which is denoted by $d_c$ in this paper, and weight coefficients are chosen from a finite weight set, $\mathcal{W}_s$, with $f \geq d_c$ positive real members, as follows:

$$\mathcal{W}_s = \{w_i \in \mathbb{R}^+ | i = 1, 2, ..., f\},$$

where $\mathbb{R}^+$ is the set of positive real numbers and $\sigma_w^2 \triangleq \frac{1}{f} \sum_{j=1}^{f} w_j^2$ is defined as the average weight set energy. Let $g_{i,j}$ denote the weight coefficient assigned to the $j^{th}$ modulated information symbol in generating the $i^{th}$ coded symbol. It is clear that $g_{i,j} \in \mathcal{W}_s$, if $b_j$ is selected in generating $c_i$; otherwise $g_{i,j} = 0$. Let $G_{m \times k}$ denote the matrix of weight coefficients, referred to as the generator matrix, where the $j^{th}$ element in the $i^{th}$ row of $G$ is $g_{i,j}$, then AFC encoding process can be shown as a matrix form as follows:

$$u = Gb',$$

where $u$ is a $m \times 1$ vector of coded symbols and $m$ is the number of coded symbols. By considering information and coded symbols as variable and check nodes, respectively, the encoding process of AFC can be further described by a weighted bipartite graph as in Fig. 2.

As shown in [9], if information symbols are selected uniformly at random in the encoding process of an AFC, some information symbols may not have connections to any coded symbol even with a large number of coded symbols, which leads to a decoding error floor. To avoid such an error floor, we have proposed a modified encoder for AFC by maximizing the minimum variable node degree. This way, to generate each coded symbol, $d_c$ information symbols are randomly selected among those which currently have the smallest degrees. The entire data is also precoded using a high rate LDPC code, which has shown to significantly reduce the error floor in AFC codes [9]. Further details of AFC code design can be found in [9].

#### B. Multiple Access Analog Fountain Codes

Each coded symbol in AFC is a linear combination of modulated information symbols with real weight coefficients. Thus, the sum of two or more AFC coded symbols is still an AFC coded symbol with a larger degree. This motivates us to consider AFCs in a multiple access scenario, where the sum of coded symbols from various users is received at the destination; thus, forming an equivalent AFC code at the destination.

In the proposed scheme, referred to as multiple access analog fountain code (MA-AFC), each active user $U_j$ uses an AFC with degree $d_j \geq 1$ and a weight set $\mathcal{W}_j$ to generate a potentially limitless number of AFC coded symbols. Let $u_{i,j}$
denote the vector of coded symbols generated by $U_j$, and $G_{m \times k}$ denote $U_j$'s generator matrix, where $m$ is the number of coded symbols. Then at time instant $i$, the received signal at the destination, $y_i$, is given by:

$$y_i = \sum_{j \in S} h_j u_i^{(j)} + n_i,$$

(5)

According to (4), we have $u_i^{(j)} = \sum_{t=1}^{k} g_i^{(j)} b_t^{(j)}$; thus, (5) can be rewritten as follows:

$$y = \sum_{j \in S} h_j G^{(j)} b^{(j)}' + n,$$

(6)

where $b^{(j)}$ is the information sequence of $U_j$. Eq. (6) can be further simplified as follows:

$$y = G b' + n,$$

(7)

where $G \triangleq [h_1 G^{(1)} h_2 G^{(2)} ... h_N G^{(N)}]$ and $b \triangleq [b^{(1)} b^{(2)} ... b^{(N)}]$. This clearly shows that the received signal at the destination can be seen as a coded symbol of an equivalent AFC, where modulated information symbols are chosen from all active users. It is important to note that the weight coefficients of the equivalent AFC are the weight coefficients of the original AFC codes at each user, multiplied by the gain of the respective channel. More specifically, the equivalent weight set at the destination can be shown by $W_e \triangleq \cup_{i \in S} \{h_i W_s\}$ and the code degree $d_e$ of the equivalent AFC code at the destination is $d_e \triangleq \sum_{i \in S} d_i$. Fig. 3 and Fig. 4 show the original AFC code at each user and the equivalent bipartite graph of the AFC code at the destination, respectively, when the number of users is 2, i.e., $M = 2$.

C. Weight Set Design for MA-AFC

As mentioned before, to achieve the capacity of the Gaussian MAC, the output signal distribution of each user should follow the Gaussian distribution. In this section, we propose an optimization problem to find the optimum weight set in order to guarantee that AFC coded symbols from each user follow the Gaussian distribution.

Let us consider an AFC with the code degree $d_e$, where information symbols are selected uniformly at random to generate each coded symbol. For a coded symbol $u_i$, and a given real number $c$, we have

$$p(u_i = c) = p\left(\sum_{t \in \mathcal{M}(i)} g_{i,t} b_t = c\right),$$

(8)

where $\mathcal{M}(i)$ is the set of variable nodes connected to the check node $u_i$. Since each information symbol is either -1 or 1 with the same probability of 0.5, and weights are randomly chosen from $\mathcal{W}$, then $s_{i,t} \triangleq g_{i,t} b_t$ is uniformly distributed as follows:

$$p(s_{i,t} = v) = \frac{1}{2f}, \quad |v| \in \mathcal{W}_s.$$  

(9)

Furthermore, the mean and variance of $s_{i,t}$ are respectively, $m_s = 0$ and $\sigma^2_s = \frac{1}{f} \sum_{t=1}^{d_i} (w^2_t) = \sigma^2_w$. Since $s_{i,t}$'s are identical and independent random variables, $u_i$ has mean 0 and variance $d_e \sigma^2_w$. Moreover, when $d_e$ is relatively large, according to the central limit theorem, $u_i$ has zero mean Gaussian distribution with variance $d_e \sigma^2_w$. However, for a small value of $d_e$, we need to find the optimum weight set in order for the signal distribution to approach the Gaussian distribution. Therefore, we need to find the weight coefficients such that the following condition is satisfied, for a given $\epsilon > 0$ and $\delta > 0$:

$$|p_{i,\delta}^{(i)} - q_{i,\delta}^{(i)}|^2 \leq \epsilon, \quad \text{for } i = 1, 2, ..., i_{\text{max}}$$

(10)

where $p_{i,\delta}^{(i)} \triangleq p\left((i-1)\delta \leq \sum_{j=1}^{d_i} b_j w_j < i\delta\right)$, $q_{i,\delta}^{(i)} \triangleq Q\left((i-1)\delta\right) - Q(i\delta)$, $i_{\text{max}}$ is chosen to be large normally larger than 10, and $Q(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-z^2/2} dz$. It is clear that when condition (10) is satisfied, the output signal distribution will be close to the Gaussian distribution with at most $\sqrt{\epsilon}$ difference at $\delta$-distanced signal points. This optimization problem can be numerically solved for different values of $\delta$ and $\epsilon$. For instance, for $f = 8$, $\delta = 0.2$ and $\epsilon = 10^{-4}$, the optimum weight set is as follows: $\{\frac{1}{7}, \frac{1}{7}, \frac{1}{7}, \frac{1}{7}, \frac{1}{7}, \frac{1}{7}, \frac{1}{7}, \frac{1}{7}\}$. Since the sum of Gaussian distributed signals is still Gaussian, the distribution of MA-AFC coded symbol is also Gaussian as long as AFC coded symbols of each active user follows a Gaussian distribution.

IV. DECODING OF MA-AFC

Let us consider the bipartite graph of a MA-AFC in Fig. 4. The optimum decoding algorithm for MA-AFC produces the posteriori probability distribution of $b$, i.e., $P(b|y,G)$, which is a sufficient statistic for $b$ in an information theoretic sense, where $y = Gb + n$ as in (7). Here, we present the belief propagation (BP) decoding algorithm for a MA-AFC and then an asymptotic performance analysis of the BP decoder is presented.

A. Belief Propagation Decoding of MA-AFC

Belief propagation (BP) is an efficient message passing algorithm for estimating the marginal posterior distribution based on the observations. In each iteration of BP, messages are first transmitted from variable to check nodes and then new
messages are generated at each check node to be sent back to each of its connected variable nodes.

As variable nodes are binary, then the common choice for the messages is the log-likelihood ratio (LLR) \( L_{r \rightarrow t}(t) \) where \( L_{r \rightarrow t}(t) \) represent the message from variable node \( b_r \) to check node \( y_t \) and \( L_{t \rightarrow r}(t) \) represents the message in the reverse direction at the \( t \)-th iteration of the BP algorithm. The updating rules for the BP algorithm at the \( t \)-th iteration \( (t \geq 1) \) can then be shown as follows \([11]\):

\[
L_{t \rightarrow r}^{(t)} = \log \frac{P\{y_t | b_r = +1, G_r \}}{P\{y_t | b_r = -1, G_r \}} \sum_{r' \in \mathcal{N}(r) \setminus \ell} L_{r' \rightarrow t}^{(t)},
\]

where \( \mathcal{N}(r) \setminus \ell \) is the set of all variable nodes connected to check node \( y_t \) except variable node \( b_r \) and \( \mathcal{N}(r) \setminus \ell \) is the set of all check nodes connected to variable node \( b_r \) except check node \( y_t \). By considering that the noise variance is 1, we have

\[
P\{y_t | b_r = x, G_r \} = \sum_{(b_r,r') \in \mathcal{M}(t)} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2} (s_r - \sum_{r' \in \mathcal{N}(r) \setminus \ell} g_{r',r} b_{r'})^2} \prod_{r' \in \mathcal{M}(t)} p_X(b_{r'}), (11)
\]

where \( x \in \{-1, +1\} \) and \( p_X(b_r = +1) \propto \exp(L_{t \rightarrow r}^{(t)}) \). The initial messages \( L_{r \rightarrow t}^{(0)} \) correspond to prior LLRs of modulated information symbols, which is 0 due to the fact that information symbols are equally probable binary random variables. These iterations are repeated until a specific number of iterations are performed or convergence is achieved. After a predefined number of iterations, \( T \), the final value of LLRs can be calculated as \( L_{r \rightarrow t}^{(T)} = \sum_{t' \in \mathcal{N}(r) \setminus \ell} L_{t' \rightarrow r}^{(T)} \). A variable node \( b_r \) is then decoded as 1, if \( L_{r \rightarrow t}^{(T)} > 0 \); otherwise, it is decoded as 0.

B. Asymptotic Performance Analysis of MA-AFC based on the BP Decoding

A commonly used analytical tool for analyzing a BP decoder is density evolution, which calculates the evolutions of message passing in the iterative decoding process. In this paper, we focus on the density evolution analysis in the asymptotic case, when the number of variable and check nodes go to infinity.

Let us refer to information symbols of \( U_i \) as Type-\( X_i \) variable nodes in the bipartite graph of a MA-AFC code, for \( i = 1, 2, ..., N \). The following lemma gives an approximation of LLRs for various types of variable nodes in each iteration of the BP decoder in the asymptotic case, when the number of variable and check nodes are very large.

**Lemma 1:** Let \( L_{X_i \rightarrow t}^{(t)} \) denote the message passed from a Type-\( X_i \) variable node to a check node \( y_t \) in the \( t \)-th iteration of the BP decoding algorithm. Then, \( L_{X_i \rightarrow t}^{(t)} \) can be approximated by a normal random variable with mean \( m_{i,t}^{(t)} \) and variance

\[
2m_{i,t}^{(t)} = h_i^2 \sigma_w^2 \frac{d_i m}{k} \left( \frac{2}{1 + \sigma_Y^2} \right), (13)
\]

where \( \sigma_Y^2 = \sum_{j \in S} h_i^2 h_j^2 \sigma_w^2 S_m j + S(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} (1 - \tanh(x - y\sqrt{x})) e^{-x^2/2} dx \). The proof of this lemma is provided in Appendix A. The BER for each device after \( t \) iterations of the BP decoder can then be calculated as \( Q \left( \sqrt{m_{i,t}^{(t)}} \right) \). Let \( P_{r,i} \) denote the BER of \( U_i \) at the destination, then by using Lemma I and for \( i, j \in S \), we have:

\[
\frac{m_{i,t}^{(t)}}{m_{j,t}^{(t)}} = \frac{h_i^2 d_i}{h_j^2 d_j}. (14)
\]

Accordingly, we have:

\[
P_{r,i} = Q \left( Q^{-1}(P_{r,j}) \left( \frac{h_i^2 d_i}{h_j^2 d_j} \right) \right). (15)
\]

This shows that an active user with a higher product of channel gain and code degree, has a lower BER compared to other active users; thus, can be decoded sooner at the destination.

V. SIMULATION RESULTS

For simulation purposes, we consider \( k = 1000 \) and a AFC code with the weight set \( W_s = \{1/2, 1/3, 1/5, 1/7, 1/11, 1/13, 1/17, 1/19\} \). Let us first investigate a 2-user MAC, where the users use AFC with the same weight set. The channel gain and code degree for both users are \( h_1 = h_2 = 1 \) and \( d_1 = d_2 = 4 \), respectively. Fig. 5 shows the sum-rate achieved by the MA-AFC approach versus the received SNR at the destination. The target BER is \( 10^{-4} \).

As can be seen in Fig. 5, MA-AFC can closely approach the Shannon’s Limit when the received SNR at the destination, \( d \), is very high.

Accordingly, we have:

\[
P_{r,i} = Q \left( Q^{-1}(P_{r,j}) \left( \frac{h_i^2 d_i}{h_j^2 d_j} \right) \right). (15)
\]

This shows that an active user with a higher product of channel gain and code degree, has a lower BER compared to other active users; thus, can be decoded sooner at the destination.

![Fig. 5. Achievable sum-rate of MA-AFC approach versus the received SNR at the destination. The target BER is 10^{-4}.](image-url)
which has the highest channel gain has a lower BER compared to other users. Furthermore, U₁ has the highest BER as it has the lowest product of channel gain and code degree amongst various users. This validates the results of Lemma 1 as the user with the larger of the product of channel gain and code degree will have the lowest BER at the destination. The average BER for each user obtained from the density evolution analysis in Lemma 1 is also shown in Fig. 6 which is very close to the simulation results.

VI. CONCLUSIONS

In this paper, we proposed a novel rateless multiple access scheme based on capacity-approaching analog fountain codes to approach the sum-rate capacity of the multiple access channel in a wide range of SNRs. In the proposed scheme, all users utilize the same AFC code to transmit at the same time and the same channel; thus, forming an equivalent analog fountain code at the destination. The destination then performs joint decoding to recover all users’ information symbols. We further analyzed the proposed multiple access analog fountain code by using the density evolution technique. Simulation results show that the proposed approach can approach the sum-rate capacity of the Gaussian multiple access channel in a wide range of SNRs.

APPENDIX A
PROOF OF LEMMA II

Let us first define Y_j \triangleq \sum_{r' \in \mathcal{M}(j)} r' g_{j,r'} b_{r'} as the j^{th} coded symbol without the r^{th} information symbol. In (11), it has been shown that the LLR passed from check node y_j to variable node b_r in the t^{th} iteration of the BP algorithm, \( L_{j \rightarrow r}^{(t)} \), can be approximated as follows:

\[
L_{j \rightarrow r}^{(t)} = 2 f_j(y_j) g_{j,r},
\]

where \( f_m(y) \) is defined as follows for \( m \in \{0, 1\} \):

\[
f_m(y) = \sum_{r' \in \mathcal{M}(j) \backslash r} \frac{1}{2 \pi \sigma r^2} e^{-\frac{1}{2}(y-Y_j)^2} \times (y - Y_j)^m \prod_{r'' \in \mathcal{M}(j) \backslash r} p_X(b_{r''}).
\]

Furthermore, the mean and variance of \( L_{r \rightarrow \ell}^{(t)} \) can be calculated as follows (11):

\[
|E \{ L_{r \rightarrow \ell}^{(t)} \}| = 2 \int_{-\infty}^{\infty} f_r(y) f_\ell(y) dy \sum_{\ell' \in \mathcal{N}(r) \backslash \ell} g_{r,r'}^2 (16)
\]

var \{ L_{r \rightarrow \ell}^{(t)} \} = 2|E \{ L_{r \rightarrow \ell}^{(t)} \}|. (17)

Moreover, when the number of variable and check nodes go to infinity, the integral part of (16) tends to \( \frac{1}{|1 + \sigma_Y^2|} \) (11), where \( \sigma_Y^2 \) is the variance of \( Y_j \). It has been shown that in the asymptotic case, \( L_{r \rightarrow \ell}^{(t)} \) is normally distributed with the mean and variance calculated in (16) and (17), respectively. More specifically, for a Type-X, variable node, (16) can be rewritten as follows:

\[
m_1^{(t)} \triangleq |E \{ E_{X_1 \rightarrow \ell}^{(t)} \}| = \frac{2}{|1 + \sigma_Y^2|} h_r^2 \sum_{\ell' \in \mathcal{N}(X_1) \backslash \ell} g_{\ell' X_1}^2. (18)
\]