Compute-and-Forward using nested linear codes for the Gaussian MAC

Jingge Zhu and Michael Gastpar, Member, IEEE

Abstract—The classical modulo-lattice construction of Erez et al. has been successfully applied to several coding problems under Gaussian noise, including coding for computation over multiple-access channels (MAC). For the latter problem, an alternative construction can be developed by extending a recently proposed nested linear code to Gaussian case. In this note, it is shown that using the nested linear code with judiciously chosen input distributions, the original compute-and-forward result is recovered and larger computation rates are achievable. In particular we show that the Gaussian input distribution is not optimal in general for the computation problem over Gaussian MAC. Among other results, new achievable rates for the Gaussian two-way relay channel (TWRC) are given.

I. INTRODUCTION

It is widely known that in a communication network, messages should be mixed and processed in the intermediate nodes in order to obtain the best throughput. An excellent example is Network Coding where this idea is demonstrated in noiseless networks. For a noisy network, computations in intermediate nodes are as important but much less understood. In this note we consider the computation problem in a Gaussian network in its simplest form, namely decoding the sum of two codewords on a 2-user Gaussian MAC of the form

\[ y = x_1 + x_2 + z \tag{1} \]

with \( y, x_k \in \mathbb{R}^n \) denoting the channel output at the receiver and channel input of transmitter \( k = 1, 2 \). Both users are assumed to have the power constraint \( \mathbb{E} \| x_k \|^2 \leq nP \). The white Gaussian noise with unit variance per entry is denoted by \( z \in \mathbb{R}^n \). User \( k \) uses codebook \( C_k \) and its codewords are denoted by \( u_k \in \mathbb{R}^n \) where \( q \) is a prime number. The channel input \( x_k \) is generated using codewords \( u_k \) in a way specified later. The rate of the codebook is defined as \( R_k = \frac{1}{n} \log |C_k| \).

The goal of the receiver is to decode the sum of two codewords \( s := u_1 \oplus u_2 \) from the channel output \( y \) where the sum is performed component-wise in the finite field. Let \( \hat{s} \) denote the decoded sum. The error event is defined as

\[ P_{e,\text{sum}}^{(n)} := P(\hat{s} \neq s) \tag{2} \]

where \( n \) is the length of codewords.

Definition 1 (Computation rate pair): Consider a 2-user Gaussian MAC in (1). We say a computation rate pair \((R_1^*, R_2^*)\) with respect to a sum is achievable if it holds that for any \( \epsilon > 0 \), there exists codebooks \( C_k \), such that the sum decoding error probability in (2) satisfies \( P_{e,\text{sum}}^{(n)} < \epsilon \) for large enough \( n \), whenever the rate \( r_k \) of the codebook \( C_k \) satisfies \( r_k < R_k^* \) for \( k = 1, 2 \).

In this paper we will only focus on the simple case when \( R_1^* = R_2^* \), which we call the symmetric computation rate. The compute-and-forward scheme achieves the following symmetric computation rate.

Theorem 1 (Compute-and-forward [1]): For the 2-user Gaussian MAC in (1), the symmetric computation rate

\[ R_{CF}^S(P) := \frac{1}{2} \log(1/2 + P) \tag{3} \]

is achievable. With power allocations

\[ \alpha R_{CF}^S(P/\alpha) = \frac{\alpha}{2} \log(1/2 + P/\alpha) \tag{4} \]

is achievable for any \( \alpha \in [0, 1] \).

Remark 1: The rate (3) is given in [1]. By using only \( \alpha \) fraction of the transmission time with power \( P/\alpha \), we obtain (4) which is better than the former rate with a maximizing \( \alpha \).

Although asymptotically optimal in the high SNR regime, the result in the low SNR regime can be improved using a simple separation scheme. Namely let the receiver decode both codewords and add them up.

Proposition 1 (Separation): For the 2-user Gaussian MAC in (1), an achievable symmetric computation rate is

\[ R_{SEP}^S(P) := \frac{1}{4} \log(1 + 2P) \tag{5} \]

Comparing to the upper bound \( \frac{1}{2} \log(1 + P) \), this achievable computation rate is good at low SNR but suboptimal at high SNR regime. We can further improve the rate by time-sharing the two above schemes.

Proposition 2 (Time-sharing): For any \( P_1, P_2 \geq 0, \beta \in [0, 1], \alpha \in [0, 1] \) such that \( \beta P_1 + (1 - \beta)P_2 = P \), an achievable symmetric computation rate for the Gaussian MAC in (1) is

\[ R_{TS}^S(P) := \beta \alpha R_{CF}^S(P_1/\alpha) + (1 - \beta)R_{SEP}^S(P_2) \tag{6} \]

where \( R_{CF}^S, R_{SEP}^S \) are defined in (3) and (5).

In the following we show that with the idea of nested linear codes [2], we can give an alternative codes construction for the compute-and-forward scheme. This construction recovers the original compute-and-forward result and more importantly, it improves upon the best known results.
II. SUM DECODING WITH NESTED LINEAR CODES

We first briefly describe the nested linear codes studied in [2]. Given a random variable $X$, let $T^{(n)}(X)$ denote the typical set [3, Ch. 2.4] of the distribution of $X$.

- **Codebook generation**: Select a random variable $U_k$ defined on $\mathbb{F}_q$ with $q$ a prime number. Generates two matrices $H \in \mathbb{F}_q^{n \times t}$, $G \in \mathbb{F}_q^{n \times q}$ and two vectors $d_k \in \mathbb{F}_q^t$ whose entries are chosen i.i.d. uniformly from $\mathbb{F}_q$. For all $w_k \in \mathbb{F}_q^t$, user $k$ tries to find some $a_k \in \mathbb{F}_q^t$ and form $u_k = Hw_k \oplus Ga_k \oplus d_k$ such that $u_k \in T^{(n)}(U_k)$. If this is possible, this $u_k$ is included in the codebook $C_k$ as the codeword for the message $w_k$, otherwise an error occurs.

- **Generating channel inputs**: User $k$ selects a random variable $X_k$ according to $T_X^{(n)}$ defined on $\mathbb{F}_q$ with $q$ a prime number. The function $X_k$ is defined as the $i$-th entry of $u_k$ for $i = 1, \ldots, n$.

- **Decoding**: Define $u(w, a) := Hw \oplus Ga \oplus d_1 \oplus d_2$. Given the channel output $Y$, the decoder finds a unique $w$ such that $(y, u(w, a)) \in T^{(n)}(Y, U_1 \cup U_2)$ for some $a$. The estimated sum codeword is then formed as $\hat{u} = u(w, a)$.

With the procedure above we can show the following result.

**Theorem 2**: Consider the 2-user MAC in (1). Let random variables $U_1, U_2$ have the same distribution $p_U$ over the finite field $\mathbb{F}_q$ with a prime $q$. The symmetric computation rate

$$R^S_{NL}(P) := I(U_1 \oplus U_2; Y) - H(U_1 \oplus U_2) - H(U_1) \quad (7)$$

is achievable where $X_k \in \mathbb{R}$ is generated through a conditional probability distribution $p_{X_k|U}$ satisfying $E[|X_k|^2] \leq P$.

**Proof**: The main idea of the construction can be found in [2, Thm. 1], which deals with a joint source-channel coding problem. A proof of this theorem can be deduced from [4] for the case when $Y$ is a discrete random variable. Using a quantization argument on $Y$ as in [3, Ch. 3], it is straightforward to extend the result for the Gaussian case with continuous output alphabet.

For simplicity of presentation, we will represent the elements in the finite field $\mathbb{F}_q$ using the set $\mathbb{U} := \{-(q-1)/2, \ldots, (q-1)/2\}$

The sum of two elements is given by $U_1 \oplus U_2 := (U_1 + U_2) \mod q$, i.e., the usual modular arithmetic for integers. We also define $\mathbb{U}^+ := \{1, \ldots, (q-1)/2\}$ and $\mathbb{U}^- := \{-(q-1)/2, \ldots, -1\}$.

III. ACHIEVABLE SYMMETRIC COMPUTATION RATE

The achievable computation rate given in Theorem 2 depends on the conditional distribution $p_{X_k|U}$ which we have the freedom to choose according to the channel in consideration. For the Gaussian MAC, we study a simple (deterministic) function which takes the form

$$X_k = U_k \cdot \Delta \text{ for } k = 1, 2$$

with some real number $\Delta > 0$ satisfying the power constraint

$$\sum_{u} \frac{p_U(u)}{\Delta^2} = P. \quad (10)$$

Given the distribution of $U_1, U_2$, we need the distribution of $U_1 \oplus U_2$ and the equivalent channel from $U_1 \oplus U_2$ to $Y$ in order to evaluate the expression in Theorem 2.

**Proposition 3**: Assume $U_1, U_2$ have the distribution $p_U$ over the finite field $\mathbb{F}_q$ represented using the set $\mathbb{U}$ in (8). Define $S := U_1 \oplus U_2$ and

$$A(s) := \sum_{i=-(q-1)/2}^{(q-1)/2} p_U(i)p_U(s - i - q)$$

$$B(s) := \sum_{i=-(q-1)/2}^{(q-1)/2} p_U(i)p_U(s - i)$$

$$D(s) := \sum_{i=-(q-1)/2}^{(q-1)/2} p_U(i)p_U(s - i)$$

$$E(s) := \sum_{i=-(q+1)/2}^{(q+1)/2} p_U(i)p_U(s - i + q).$$

The distribution of $S$ is given by

$$p_S(s) = A(s) + B(s)$$

for $s \in \mathbb{U}^+ \cup \{0\}$ and

$$p_S(s) = D(s) + E(s)$$

for $s \in \mathbb{U}^-$. If $X_k$ is generated as in (9), the conditional density function $f_{Y|S}$ is given by

$$f_{Y|S}(y|s) = \frac{A(s)}{p_S(s)} N(y; \Delta(s - q), 1) + \frac{B(s)}{p_S(s)} N(y; \Delta s, 1)$$

for $s \in \mathbb{U}^+$,

$$f_{Y|S}(y|s) = \frac{D(s)}{p_S(s)} N(y; \Delta s, 1) + \frac{E(s)}{p_S(s)} N(y; \Delta(s + q), 1)$$

for $s \in \mathbb{U}^-$ and

$$f_{Y|S}(y|0) = N(y; 0, 1)$$

where $N(y; m, \sigma^2) := \frac{1}{\sqrt{2\pi}\sigma^2} e^{-(y-m)^2/(2\sigma^2)}$.

**Remark 2**: The proof is straightforward but omitted for the sake of space. In fact the distribution $p_S$ is the circular convolution of $p_U$ with period $q$. It is easy to show that if $p_U$ is symmetric, i.e., $p_U(u) = p_U(-u)$ for $u \in \mathbb{U}$, $p_S$ is also symmetric.

The achievable computation rate in Theorem 2 can be readily evaluated for any given distribution $p_U$. We give a few examples in the sequel.
Example 1 (Uniform distribution): We assign a uniform distribution to $U_1, U_2$, i.e., $p_U(u) = 1/q$ for all $u \in U$. It is easy to see that $S$ is also uniformly distributed in $U$. We can find $f_{Y|S}$ using Proposition 3 and evaluate the achievable rates using Theorem 2. Figure 1 shows the achievable rates with different choices of $q$. Notice that in this case $H(U_1 \oplus U_2) = H(U_1) = \log q$ hence $R_{NL}^N$ is always positive.

In high SNR regime, we can show that the rate only scales as $1/2 \log \frac{\pi P}{\pi e}$ due to the shaping loss.

\begin{align}
\text{Example 2 (Discretized Gaussian distribution): In this example we show that a proper choice of the distribution on $U$, the compute-and-forward result in Theorem 1 can be recovered using Theorem 2. Given a prime number $q$ and $A > 0$, we consider the following distribution on $U$

$p_U(u) = \frac{1}{\alpha(q-1)/2} e^{-\frac{(\Delta u)^2}{2A}}$ (11)

with

$\alpha(q-1)/2 := \sum_{u=-\frac{q}{2}}^{\frac{q}{2}-1} e^{-\frac{(\Delta u)^2}{2A}}$

and $\Delta$ is chosen such that (10) is satisfied. In this example we will only focus on the limits

$q \to \infty, \Delta \to 0$ and $q\Delta^2 \to \infty$ (12)

with which $p_U$ approaches a Gaussian distribution.

Proposition 4 (Discretized Gaussian): Consider the 2-user Gaussian MAC in (1). Let $p_U$ be the distribution given in (11) and choose $A = P$. In the limits of (12), we have the achievable symmetric computation rate

$R_{NL}^N = \frac{1}{2} \log (1/2 + P)$ (13)

where $R_{NL}^N$ is given in (7).

Proof sketch: In this proof we use natural logarithm for simplicity. Choosing $p_U$ in (11), the entropy of $U_1$ is calculated to be

$H(U_1) = \log \alpha(q-1)/2 + \frac{1}{2}$ (14)

We set $A = P$ and use the lower bound on $\alpha(q-1)/2$ in Lemma 1 in Appendix to obtain:

$H(U_1) > \log (\sqrt{2\pi P} - (1 + \epsilon)\Delta) - \log \Delta + 1/2$ (15)

where $\epsilon \to 0$ in the limits (12). In Appendix Lemma 2 we show that the distribution $p_S$ of $S := U_1 \oplus U_2$ approaches a discretized Gaussian distribution with power $2P$, i.e.

$p_S(s) \rightarrow \frac{\Delta}{\sqrt{4\pi P}}e^{-\frac{(s-\Delta)^2}{2\Delta^2}}$ (16)

hence we have [5, Ch. 8]

$H(S) \rightarrow \frac{1}{2} \log (4\pi eP) - \log \Delta$ (17)

It is also shown in Appendix Lemma 2 that the channel $f_{Y|S}$ approaches a point-to-point Gaussian channel in the limits (12)

$f_{Y|S}(y|s) \rightarrow \frac{1}{\sqrt{2\pi}} e^{-\frac{(y-s)^2}{2\Delta^2}}$ (18)

hence we have [3, Ch. 3]

$I(Y; S) \rightarrow \frac{1}{2} \log (1 + 2P)$ (19)

This is expected because as pointed out in Remark 2, the distribution $p_S$ is a circular convolution of $p_U$. In the limit (12), the circular convolution approaches a usual convolution because the support size of $U$ tends to infinity and the convolution of two Gaussian distributions is Gaussian. Finally we have our achievable computation rate

$R = I(Y; S) - H(S) + H(U)$

$> I(Y; S) - H(S) + \log (4\pi eP - (1 + \epsilon)\Delta \sqrt{\epsilon}) - \log \Delta$

$\rightarrow \frac{1}{2} \log (1/2 + P)$

in the limit (12).

Example 3 (Achievable rates with optimized distributions): In this example we show that new achievable rates can be obtained with good input distributions. They are in general better than $R_{CE}^N$ in (4) and are better than $R_{SP}^N$ in (5) when SNR exceeds a certain value. For example choosing $q = 3$ and $U = \{ -1, 0, 1 \}$ gives

$p_U(0) = p_0$ (20a)

$p_U(1) = p_U(-1) = (1 - p_0)/2 := p_1$. (20b)

To satisfy the power constraint, the constant $\Delta$ is chosen to be $\Delta = \sqrt{P/(1 - p_0)}$ and $X_k$ takes values in the set $\{ -\Delta, 0, \Delta \}$. Using Proposition 3, it is easy to calculate the distribution on $S := U_1 \oplus U_2$

$p_S(0) = p_0^2 + 2p_1^2$

$p_S(1) = p_S(-1) = 2p_0p_1 + p_1^2$

and density function for the equivalent channel from $S$ to $Y$

$f_{Y|S}(y|0) = N(y; 0, 1)$

$f_{Y|S}(y|1) = \frac{p_1^2}{p_S(1)} N(y; -2\Delta, 1) + \frac{2p_0p_1}{p_S(1)} N(y; \Delta, 1)$

$f_{Y|S}(y|-1) = \frac{p_1^2}{p_S(-1)} N(y; 2\Delta, 1) + \frac{2p_0p_1}{p_S(-1)} N(y; -\Delta, 1)$

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{fig1.png}
\caption{Achievable computation rate $R_{NL}^N$ with uniform input distribution and different $q$. It is interesting to notice that for the low SNR regime, the uniform distribution with a smaller $q$ results in a better rate than a larger $q$.}
\end{figure}
This can be extended directly to other values of $q$. To evaluate the achievable rate, a procedure based on the classical Blahut-Arimoto algorithm is developed in [6] to find the optimal distribution $p_U$ which maximizes $R^*_N$. Figure 2a shows that in low SNR regime, the nested linear codes with even a small value of $q$ can outperform the compute-and-forward scheme in Theorem 1, which, according to Proposition 4, is equivalent to choosing a Gaussian distribution for nested linear codes. This in particular implies that a (discretized) Gaussian distribution is in general suboptimal for the computation problem. The choice of power $P = 1.5$ is interesting with which the two known schemes give the same computation rate $R^*_C = R^*_S = 0.5$ bit and the optimized compute-and-forward gives $R^*_C(\alpha^*) \approx 0.5020$ bit. The linear nested code gives a rate about 0.5112 bit with $q = 3$ and a rate about 0.5120 bit with $q = 11$. We do not have a complete characterization of the optimal input distribution. In the limit when $P$ approaches zero, we have the following observation.

**Proposition 5:** In the limit $P \to 0$, the optimal distribution $p_U$ with the channel input mapping (9) which maximizes $R^*_N$ in (7) approaches a Delta function, i.e., $p_U(0) = 1 - \sigma$ where $\sigma \to 0$ as $P \to 0$.

**Proof sketch:** First observe that as $P \to 0$, we have $I(U_1 \oplus U_2; Y) \to 0$ hence the optimal distribution should satisfy the property $H(U_1 \oplus U_2) - H(U_1) \to 0$. However this is only possible if $p_U$ either approaches a uniform distribution (or $p_U$ is a uniform distribution) or approaches a Delta function with all its mass on $u = 0$. We show that the uniform distribution cannot be optimal. Starting with a uniform distribution $p_U(u) = 1/q$ for all $u \in U$, we consider the perturbation $p_U(u) = 1/q + \delta$, $p_U((q-1)/2) = p_U(-(q-1)/2) = 1/q - \delta$ with small $\delta > 0$. Let $R^*_N(P, \delta)$ denote the achievable computation rate in (7) with the power $P$ and a uniform input distribution with perturbation $\delta$, we have the approximation

$$R^*_N(P, \delta) \approx R^*_N(0, 0) + P \frac{\partial R^*_N}{\partial P}(0, 0) + \delta \frac{\partial R^*_N}{\partial \delta}(0, 0)$$

for small $P$ and $\delta$. We can show that $\frac{\partial R^*_N}{\partial \delta}(0, 0)$ is strictly positive, hence a perturbation to the uniform distribution increases the achievable rates in the limit.

Notice that the Figure 2b agrees with the above observation. As SNR decreases, the optimal value $p_0$ approaches 1. Equivalently the optimal distribution $p_U$ approaches the Delta function.

**IV. APPLICATION ON THE GAUSSIAN T-WRC**

The above result has immediate application on the Gaussian T-WRC. In the symmetric setting when two transmitters have power $P$ and the relay has power $P_R$, the best known symmetric rate is

$$\min \{ R^*_T(P), \frac{1}{2} \log(1 + P_R) \}$$

with $R^*_T(P)$ defined in (6). Theorem 2 shows the possibility of increasing the first term in the min expression. Namely we can achieve the symmetric rate

$$\min \{ \hat{R}^*_T(P), \frac{1}{2} \log(1 + P_R) \}$$

where $\hat{R}^*_T(P) := \beta \alpha R^*_N(P_1 / \alpha) + (1 - \beta) R^*_S(P_2)$ for any $\alpha, \beta \in [0, 1]$, $P_1, P_2 \geq 0$ satisfying $\beta P_1 + (1 - \beta) P_2 = P$. Since we can always ensure $R^*_N > R^*_S$ by choosing the optimal input distribution $p_U$, we will obtain a higher rate $\hat{R}^*_T(P)$ than $R^*_T(P)$. However the improvement is minor.
We study the discrete random variable $U$ given in (11).

**Lemma 1 (Bounds on $\alpha$):** Let $M, A > 0$ and define

$$
\alpha_{M,A} := \sum_{i=-M}^{M} e^{-((\Delta i)^2/2A)}.
$$

We have the bounds

$$
\max\{\frac{\sqrt{2\pi A}}{\Delta} - 1 - \epsilon'_{M,\Delta} \} < \alpha_{M,A} < 1 + \frac{\sqrt{2\pi A}}{\Delta}
$$

where $\epsilon'_{M,\Delta} > 0$ depends on $M, \Delta$ in the way

$$
\epsilon'_{M,\Delta} \rightarrow 0 \text{ as } M \rightarrow \infty \text{ and } M\Delta^2 \rightarrow \infty.
$$

**Proof:** Let $S_{M,A} := \sum_{i=1}^{M} e^{-((\Delta i)^2/2A)}$, we rewrite

$$
\alpha_{M,A} = 1 + \frac{2\sqrt{2\pi A}}{\Delta} S_{M,A}
$$

The bound of $\alpha_{M,A}$ is obvious. Let $f_A(x) := \frac{1}{\sqrt{2\pi A}} e^{-\frac{x^2}{2}}$. Then $S_{M,A}$ is the right (Riemann sum of $f_A(x)$ in the interval $[0, M\Delta]$. Hence we have

$$
S_{M,A} > \int_{0}^{M\Delta} f_A(x)dx - \Delta(f_A(0) - f_A(M\Delta))
$$

$$
= \frac{1}{2} \left[ Q\left(\frac{M\Delta}{\sqrt{2A}}\right) - \frac{\Delta}{\sqrt{2\pi A}} (1 - e^{-\frac{(M\Delta)^2}{4A}}) \right]
$$

Using the bound on the $Q$-function $Q(x) < \frac{1}{2} \sqrt{\frac{2}{\pi}} e^{-x^2/2}$ we have

$$
S_{M,A} > \frac{1}{2} \frac{\Delta}{\sqrt{2\pi A}} - \frac{\sqrt{A}}{M\Delta\sqrt{2\pi}} e^{-\frac{M^2\Delta^2}{4A}} + \frac{\Delta}{\sqrt{2\pi A}} e^{-\frac{M^2\Delta^2}{4A}}
$$

and

$$
\alpha_{M,A} > \frac{\sqrt{2\pi A}}{\Delta} - 1 + (2 - \frac{2A}{M\Delta^2}) e^{-\frac{M^2\Delta^2}{4A}}
$$

The lower bound follows in the limit $M\Delta^2 \rightarrow \infty$. Similarly we have

$$
S_{M,A} < \int_{0}^{M\Delta} f_A(x)dx = \frac{1}{2} \left[ Q\left(\frac{M\Delta}{\sqrt{2A}}\right) \right]
$$

Invoking the lower bound $Q(x) > \frac{1}{1+x^2} \frac{1}{\sqrt{\frac{2}{\pi}}} e^{-x^2/2}$ we have

$$
S_{M,A} < \frac{1}{2} \frac{M\Delta\sqrt{A}}{\sqrt{2\pi A} (A + M^2\Delta^2)} e^{-\frac{M^2\Delta^2}{2A}}
$$

and hence

$$
\alpha_{M,A} < 1 + \frac{\sqrt{2\pi A}}{\Delta} - \frac{2MA}{A + M^2\Delta^2} e^{-\frac{M^2\Delta^2}{2A}}
$$

The upper bound follows directly.

**Lemma 2 (Distribution of the sum and the channel):** Let $U_1, U_2$ have the probability distribution $p_U$ in (11) and $S := U_1 \oplus U_2$. In the limit (12), the distribution of $S$ is

$$
p_S(s) = \frac{\Delta}{\sqrt{2\pi A}} e^{\frac{-s^2}{2A}} + o(\Delta)
$$

and the equivalent channel $f_{Y|S}$ in Proposition 3 is

$$
f_{Y|S}(y|s) = \frac{B(s)}{B(s) + o(\Delta)} \frac{1}{2\pi} e^{-(y-s)^2/2} + o(\Delta)
$$

**Proof sketch:** Due to the symmetry of $p_S$ we only need to consider the case $s \in \{0\} \cup U^+$. Choosing $p_U$ in (11), $A(s)$ and $B(s)$ defined in Proposition 3 can be rewritten as

$$
A(s) = \frac{\alpha_{(q-1)/2, A/2} e^{-\frac{(s-\alpha)^2}{4A}}}{\alpha_{(q-1)/2, A}}
$$

$$
B(s) = \frac{\alpha_{q-1/2, A/2} e^{-\frac{s^2}{4A}}}{\alpha_{q-1/2, A}}
$$

For $s \in \{0\} \cup U^+$, we can use Lemma 1 to show

$$
A(s) < (1 + \frac{\sqrt{\pi A}}{\Delta}) e^{-\frac{s^2}{4A}}
$$

hence $A(s) = o(\Delta)$. Implied by Lemma 1, we can write $\alpha_{M,A}$ as $\frac{\sqrt{2\pi A}}{\Delta} + a$ for some $a$ with $|a| \leq 2$ in the limit (12). With some $a_1, a_2$ with $|a_1|, |a_2| \leq 2$ and the Taylor expansion we can show

$$
\frac{A(s)}{B(s)} < \frac{\Delta}{\sqrt{\pi A} A} + \frac{A(s)}{B(s)}
$$

$$
= \frac{\Delta}{\sqrt{\pi A} A} + o(\Delta)
$$

It follows that

$$
p_S(s) = A(s) + B(s)
$$

$$
o(\Delta) + (\frac{\Delta}{\sqrt{\pi A} A} + o(\Delta)) e^{-\frac{s^2}{4A}}
$$

For the equivalent channel $f_{Y|S}$ given in Proposition 3, we can bound the ratio

$$
\frac{A(s)}{B(s)} < \frac{\Delta}{\sqrt{\pi A} A} + \frac{A(s)}{B(s)}
$$

$$
\leq \frac{\Delta}{\sqrt{\pi A} A} + \frac{\Delta^2}{\Delta^2} + o(\Delta)
$$

Hence

$$
f_{Y|S}(y|s) = o(\Delta) N(y; \Delta(s-q), 1) + \frac{B(s)}{o(\Delta) + B(s)} N(y; \Delta, 1)
$$

which proves the claim.

**References**


