arXiv:2305.04376v1 [cs.DS] 7 May 2023

交互式纠错码最大错误韧性的新上界

Meghal Gupta * Rachel Yun Zhang†加州
大学伯克利分校 麻省理工学院

2023年5月9日

摘要

在<这一style id='1'>交互式纠错码（交互式纠错码）中，Alice 和 Bob 通过交互协议进行通信，目标是由 Alice 向 Bob 传递一条消息 $x \in \{0,1\}^k$，使得即使传输的比特总数中有一部分遭到破坏，Bob 仍能确定 x。Gupta、Kalai 和 Zhang（STOC 2022年）以及 Efremenko、Kol、Saxena 和 Zhang（FOCS 2022年）的研究表明，存在能够抵御比标准非交互式纠错码更大比例错误的交互式纠错码。

研究交互式纠错码的一个主要问题是确定交互式纠错码能够实现的最优错误鲁棒性。对于比特翻转错误，已知交互式纠错码可以实现 $\frac{1}{4} + 10^{-5}$错误鲁棒性（Efremenko、Kol、Saxena 和 Zhang），而目前已知的最佳上界为$\frac{2}{7} \approx 0.2857$（Gupta、Kalai 和 Zhang）。在本研究中，我们改进了这一上界，证明任何交互式纠错码所能容忍的错误比例都不超过 $\frac{13}{47} \approx 0.2766$。

*电子邮箱：meghal@berkeley.edu。该作者获得了加州大学伯克利分校校长奖学金的资助。

†电子邮箱：rachelyz@mit.edu。本研究部分由 DARPA 根据协议编号 HR00112020023、NSF 资助项目 CNS-2154149 以及 NSF 研究生研究奖学金 2141064 资助。

目录

1 引言 **1**

2 相关工作 **2**

2.1 交互式纠错码.22.2 带反馈的纠错码.2

3 预备知识 **3**

3.1 交互式纠错码.33.2 重要引理.4

4 关于交互式纠错码最大抗噪能力的不可能性界限 **4**

4.1 攻击 1.54.2 攻击 2.64.3 攻击 3.94.4 定理证明 4.1 .11

1 引言

考虑以下任务：Alice 希望向 Bob 传递一条消息，使得即使通信比特中有固定比例遭到对手篡改，Bob 仍能保证确定她的消息。这一任务推动了对纠错码的大量研究，该研究始于 [Sha48、Ham50] 等开创性工作。纠错码将一条消息编码 x为更长的码字$\mathsf{ECC}(x)$，使得任意两个不同码字之间的汉明距离为码字长度的固定比例。为了传递消息 x，Alice 将相应的码字$\mathsf{ECC}(x)$发送给 Bob；任意两个码字之间距离较大的事实保证了对手必须篡改通信中的较大比例，Bob 才会将其错误解码为另一个码字。

纠错码研究中的一个重要问题是确定可能达到的最大错误鲁棒性，即：只要对手翻转的比特数不超过某个数值，就能保证 Bob 正确解码出 x，而这个数值可能达到的最大值是多少。事实上，许多研究都聚焦于这一问题。一般而言，错误鲁棒性参数取决于字母表大小：本文聚焦于二元字母表。众所周知，在对抗性比特翻转模型中，任何纠错码都无法抵御超过 $\frac{1}{4}$ 次篡改。

交互式纠错码。 近期，文献 [GKZ22] 提出利用交互将错误鲁棒性提升至 $\frac{1}{4}$以上。他们定义了交互式纠错码（iECC）模型如下。在交互式纠错码中，Alice 和 Bob 按照固定长度、固定顺序的协议进行交互，其中 Alice 的目标是向 Bob 传递一条消息 x。对手获得一个篡改预算，其额度为总通信量的 α 比例（其中 $\alpha > 0$）。她可以任意使用该预算（例如，全部用于正向通信，或用于正向通信和反馈通信的某种组合）。无论对手如何篡改传输的比特，目标都是让 Bob 获知 x 。

先验来看，并不清楚 交互式纠错码 是否能将错误鲁棒性提升至超过 $\frac{1}{4}$。事实上，Bob 的比特会增加相对于 Alice 前向通信量而言对手可进行篡改的额度，却没有明显的益处（因为对手可以选择将 Bob 的所有反馈篡改为对抗性字符串，从而可能弊大于利）。尽管如此， [GKZ22] 的工作首次表明，交互能够提升错误鲁棒性：他们证明，在对抗性 擦除 的情况下，交互式纠错码能够抵抗比标准（非交互式）纠错码所能抵抗的更多擦除。

对于比特翻转错误， [EKSZ22] 的后续研究首次证明了交互机制同样有助于应对比特翻转错误：其交互式纠错码能够实现对 $\frac{1}{4} + 10^{-5}$ 错误的鲁棒性，超过了任何纠错码（ECC）所能达到的最大错误鲁棒性 $\frac{1}{4}$ 。这引出了一个问题：交互式纠错码所能实现的最优错误鲁棒性是多少？

关于这个问题，目前已知的最佳上界（不可能性界）由 [GKZ22], 给出，他们证明，没有任何交互式纠错码能够抵御超过 $\frac{2}{7}$ 个对抗性错误。这个上界来自两种自然攻击的组合，其中一种无论 Alice 和 Bob 发言的轮次如何分配，都必定奏效。

攻击 1： 不篡改 Bob 的任何比特。这样一来，Bob 的消息就提供了完美可靠的反馈；在这种情况下，关于带反馈的纠错码 的研究（始于 [Ber64]）告诉我们，只需篡改 Alice 的 $\frac{1}{3}$ 比特即可。

攻击 2: 篡改一半Bob 的比特，使他的消息看起来随机，因而基本毫无用处：这样一来，Alice 的通信基本上就退化为标准

纠错码的情形；在这种情况下，对手可以篡改她的1 4 比特，让Bob 无法分辨 x 的两个可能值。

然而，问题仍然存在：一个交互式纠错码可能达到的最大错误鲁棒性是多少？是否可能实现等于这一自然上界2 7的错误鲁棒性？

在本文中，我们对后一个问题给出了否定回答，提出了一个新的上界$\frac{13}{47} \approx 0.2766$，改进了此前最优的上界 $\frac{2}{7} \approx 0.2857$。

定理 1.1（主要结果）。对于充分小的 $\epsilon > 0$，存在 $k_0 = k_0(\epsilon) \in \mathbb{N}$，使得对于任意 $k > k_0$，在二元比特翻转信道上、*Alice*试图进行通信的任何交互式纠错码都无法抵抗 $\frac{13}{47} + \epsilon$ 比例的对抗性比特翻转。

2 相关工作

本节将讨论交互式纠错码方面的先前工作，以及带反馈的纠错码方面的先前工作。

2.1 交互式纠错码

交互式纠错码的概念交互式纠错码（iECC）最早由[GKZ22], 提出，他们证明了一种能够抵抗3 5 比例的对抗性擦除的iECC，超过了标准纠错码1 2的最佳可能擦除鲁棒性。他们还给出了任意iECC擦除鲁棒性2 3 的上界。对于比特翻转错误，他们证明了任意iECC可实现的错误鲁棒性上界为2 7，从而留下了构造一种能够抵抗超过1 4 比例对抗性错误的iECC这一问题。

[GZ22] 的后续工作改进了 [GKZ22], 的擦除交互式纠错码，给出了一种具有正码率但只能抵抗6 11 次对抗性擦除的交互式纠错码构造。

在比特翻转错误模型中， [EKSZ22] 对 [GKZ22]的问题给出了肯定回答，构造出了错误鲁棒性为 $\frac{1}{4} + 10^{-5}$ 的交互式纠错码。这将任意交互式纠错码的最优错误鲁棒性范围缩小至 $[\frac{1}{4} + 10^{-5}, \frac{2}{7}]$。在本文中，我们进一步缩小了这一范围，将上界从 2 7提高至 13 47。

2.2 带反馈的纠错码

此前，人们已从带反馈的纠错码的角度研究了交互在抗噪消息通信中的应用。在带反馈的纠错码中，Alice 希望以抗错误的方式向 Bob 通信，前提是她每发送一条消息，都会收到 Bob 关于其接收内容的一些反馈。随后，她可以利用这种无噪声反馈来选择接下来发送的比特。带反馈的纠错码最早由 Berlekamp 在其博士论文中提出[Ber64] ，并在多项后续研究中得到探讨，包括[Ber68、Zig76、SW92、HKV15、GGZ22、ADL06]。最初，这种反馈是在无噪声的设定下考虑的，这意味着 Bob 的任何消息都不允许被篡改，错误率仅根据 Alice 发送的消息数量计算。也就是说，Bob 的反馈是免费的且始终正确，因此 Alice 可以针对 Bob 最需要获知的那一比特信息来定制下一条消息。

在比特翻转错误模型中， [Ber68、Zig76、SW92和HKV15] 证明，具有无噪声反馈的纠错码的最大错误鲁棒性为1 3。[GGZ22] 证明了这一界是可达到的

即使协议只在常数轮次内发送对数数量的反馈比特，也能达到这一结果。对于显式的常数轮次反馈， [BEK+22] 率先研究了擦除和错误两种情况下噪声鲁棒性与轮次复杂度之间的权衡。对于更大的字母表，最大错误鲁棒性由 [ADL06]进行了研究。

当反馈是有噪声的时，即反馈也可能遭到篡改时，相关研究成果要少得多。若干工作，例如 [BY08a、BY08b]，研究了二进制对称信道上具有有噪声反馈的纠错码。 [WQC17] 研究了对抗性破坏，其模型对正向轮次和反馈轮次分别设置了破坏预算。他们构造了一种方案，能够抵抗$\frac{1}{2}$ 的正向通信和 1 的反馈被擦除。我们注意到，他们方案的正向擦除鲁棒性等于标准纠错码所能达到的水平。

3 预备知识

记号。 本文使用以下记号：

- 对于字符串 x， $x[i]$ 表示 x 的第 i 个比特，而 $x[i\colon j]$ 表示 x 中从第 i 个比特开始、到第 j 个比特结束的子字符串。
- 对于任意 $n \in \mathbb{N}$， $[n]$ 表示整数 1，...， n。对于任意 n， $m \in \mathbb{N}$， $[n, m]$ 表示整数 n，...， m。
- 三个字符串 s_1、 s_2、 s_3 的直径 记作 $\mathrm{Diam}(s_1, s_2, s_3)$，是这三个字符串中任意两个之间的最大汉明距离。
- 多数函数记作 maj，其输入为若干比特，输出出现频率最高的比特。（如果 0 和 1 的数量相同，则输出任意一个。）

3.1 交互式纠错码

我们正式定义交互式纠错码（iECC）的概念。

定义 3.1（交互式纠错码）。 交互式纠错码（iECC）是一种非自适应交互协议[1] $\pi = \{\pi_k\}_{k\in\mathbb{N}}$，其语法如下：

- 协议开始时，*Alice* 接收某个 $x \in \{0,1\}^k$ 作为其私有输入。
- 协议结束时，*Bob* 输出某个 $\hat{x} \in \{0,1\}^k$。

我们称 π 具有 α-错误韧性，如果存在 $k_0 \in \mathbb{N}$，使得对于所有 $k > k_0$ 和 $x \in \{0,1\}^k$，以及所有至多翻转总通信量中 $\alpha \cdot |\pi|$ 的在线对抗性攻击，*Bob* 在协议结束时以概率 1输出 x 。

[1]非自适应交互协议是双方之间的一种固定长度、固定发言顺序的协议，其中每一轮由预先确定的一方向另一方发送一个比特。

3.2 重要引理

现在我们陈述一些重要的引理和组合定理。

引理 3.2。 在任意 K 个 s_1，……，$s_K \in \{0,1\}^\ell$ 字符串中，存在两个汉明距离至多为 $\left(\frac{1}{2}+\frac{1}{2(K-1)}\right)\cdot\ell$ 的字符串。

证明。 对于任意索引 $\iota \in [\ell]$，令 c_ι 表示满足 $s_j[\iota]=0$ 的字符串 s_j 的数量。那么，

$$\sum_{(i,j)\in\binom{K}{2}} \Delta(s_i,s_j) = \sum_{\iota\in[\ell]} c_\iota(K-c_\iota) \le \ell\cdot\frac{K^2}{4},$$

因此根据鸽巢原理，存在 $(i,j)\in\binom{K}{2}$ 使得 $\Delta(s_i,s_j) \le \frac{\ell\cdot K^2/4}{\binom{K}{2}} = \left(\frac{1}{2}+\frac{1}{2(K-1)}\right)\cdot\ell.$ □

定理 3.3。 *[She83]* 存在 δ_0 使得对于任意 $\delta<\delta_0$，在任意一个具有 n 个顶点且至多包含 δn^3 个三角形的无向图中，都存在一个大小为 $\frac{1}{4\delta}$ 的独立集。

推论 3.4。 对于足够小的 $\epsilon>0$，以及任意一组 K 个字符串 s_1，……，$s_K\in\{0,1\}^\ell$，存在 $\epsilon K^3/4$ 个无序三元组 (s_i,s_j,s_k)，其成员是互不相同的字符串，并且 $\mathit{Diam}(s_i,s_j,s_k)\le\left(\frac{1}{2}+\epsilon\right)\cdot\ell$。

证明。 考虑一个图，其顶点为 K 个字符串，且 s_i 与 s_j 之间有一条边，当且仅当 $\Delta(s_i,s_j)\le\left(\frac{1}{2}+\epsilon\right)\cdot\ell$。如果三角形少于 $\epsilon K^3/4$ 个，那么根据定理 3.3，存在一个大小为 $1/\epsilon$ 的独立集；根据引理 3.2，这是不可能的。 □

定理 3.5。 *(Turan，[图41])* 对于任意 $m\in\mathbb{N}$，任意一个顶点数为 $\frac{n^2}{2m}$ 且边数少于相应界限的图，都有一个大小为 m 的独立集。

推论 3.6. 对于足够小的 $\epsilon>0$，以及任意一组 K 个字符串 s_1，……，$s_K\in\{0,1\}^\ell$，至少存在 $\epsilon K^2/2$ 对无序字符串 (s_i,s_j) 满足 $\Delta(s_i,s_j)\le\left(\frac{1}{2}+\epsilon\right)\cdot\ell$。

证明。 考虑一个图，其中以 K 个字符串作为顶点，且当 s_i 和 s_j 满足 $\Delta(s_i,s_j)\le\left(\frac{1}{2}+\epsilon\right)\cdot\ell$ 时，两者之间有一条边。如果满足 $\Delta(s_i,s_j)\le\left(\frac{1}{2}+\epsilon\right)\cdot\ell$ 的无序字符串对 (s_i,s_j) 少于 $\epsilon K^2/2$，那么根据定理 3.5，存在一个大小为 $\frac{1}{\epsilon}$ 的独立集；根据引理 3.2，这是不可能的。 □

定理 3.7。 （拉姆齐，*[拉姆87]*）对于任意 m，$n\in\mathbb{N}$，存在 $R(m,n)\le\binom{m+n-2}{n-1}\in\mathbb{N}$ 使得任何至少有 $R(m,n)$ 个顶点的无向图，要么包含一个有 m 个顶点的团，要么包含一个有 n 个顶点的独立集。

4 交互式纠错码最大抗噪能力的不可能性界

本节将给出我们的主要结果：对于任意非自适应交互式纠错码，都存在一种攻击，至多包含 $\frac{13}{47}$ 次篡改，使得 Bob 猜中 Alice 的输入 x 的概率不超过 $\frac{1}{2}$。

定理 4.1。 对于足够小的 $\epsilon>0$，对于所有 $k>100\epsilon^{-4}$，不存在针对 $x\in\{0,1\}^k$ 的交互式纠错码 能够以大于 $\frac{1}{2}$ 的概率抵御超过 $\frac{13}{47}+2\epsilon$ 比例的错误。

本节余下部分将用于证明该定理。在本节中，Alice 的输入始终记为 $x \in \{0,1\}^k$。交互式纠错码的长度记为 n。

总体而言，我们的证明将按如下方式展开。我们将任意一个候选协议分为两个部分：第一部分由协议的前 $\frac{21}{47}n$ 轮组成，第二部分由剩余的 $\frac{26}{47}n$ 轮组成。在第一部分中，我们将 Alice 发送的比特数记为 A_1，将 Bob 发送的比特数记为 B_1。同样，在第二部分中，我们分别将 Alice 和 Bob 发送的比特数记为 A_2 和 B_2 。我们将在第4.1、4.2和4.3 节给出三种攻击。根据 A_1、B_1、A_2、B_2 的取值，至少有一种攻击必定成功，且至多使用13 47 次篡改。

—

在本节中，通信记录是任一方收到的比特序列。请注意，由于对手可以篡改消息，通信记录可能与 Alice 和 Bob 发送的内容不同。如果存在两个输入 x_1、$x_2 \in \{0,1\}^k$ 及相应的策略，能够至多篡改 αn 个比特，并且使 Bob 在两种情况下看到的通信记录视图完全相同，我们就称该攻击在 α 次篡改下成功。此时，Bob 猜出 Alice 的真实值 $x \in \{x_1, x_2\}$ 的概率不可能超过1 2。

–

4.1 攻击 1

在第一次攻击中，对手在协议的两个部分都采取相同的行为。她篡改 Alice 的比特而不改动 Bob 的比特，使得存在两个输入，其中 Alice 的通信被篡改的部分至多为 1 3。我们指出，这种攻击早在 [Ber64] 中就已为人所知。

引理4.2。 对于任何由 *Alice* 的 A 个比特和 *Bob* 的 B 个比特组成的协议，以及任意三个可能的输入 x_1、x_2、x_3，这三个输入中存在两个输入 y_1、$y_2 \in \{x_1, x_2, x_3\}$，以及一个通信记录$T \in \{0,1\}^{A+B}$，使得对手最多篡改 $\frac{1}{3}A+1$ 个比特后，在 *Alice* 的输入为 y_1 或 y_2 的情况下，协议的通信记录均为 T。

证明。 我们如下定义 T。

- Bob 的比特均不会被篡改，也就是说，Alice 会正确收到 Bob 发送的每一个比特。

- 对于 Alice 的比特，对手首先会将 Alice 的第 t 个比特篡改为 maj($a_t(x_1)$ $a_t(x_2)$ $a_t(x_3)$)，其中 $a_t(x_i)$ 表示 Alice 在输入为 x_i 时的第 t 个比特。对于任意 $t \in [A]$，我们用 $\delta_t(x_i)$ 表示当 Alice 的输入为 x_i 时，对手截至第 t 个比特所篡改的比特数。对手会持续进行这次攻击，直到在第 t_0 轮时，$\delta_t(x_i)$ 中第二大的值达到 $\lceil \frac{1}{3}A \rceil$；此时，她切换到以下策略：令 y_1、y_2、y_3 分别表示 x_i 中 $\delta_{t_0}(x_i)$ 最小、第二小和最大的值（因此 $\delta_{t_0}(y_2) = \lceil \frac{1}{3}A \rceil$），对手将 Alice 剩余的比特篡改为 $a_t(y_2)$，其中 $t_0 < t \leq A$。

如果点 t_0 从未发生，那么最小和第二小的 $\delta_A(x_i)$ 都小于 $\lceil \frac{1}{3}A \rceil$，问题就解决了。否则，我们声称到

协议结束时，$\delta_A(y_2) = \lceil \frac{1}{3}A \rceil$。至于 $\delta_A(y_1)$，我们有

$$\begin{aligned}
\delta_A(y_1) &\le \delta_{t_0}(y_1) + (A - t_0) \\
&\le \delta_{t_0}(y_1) + A - (\delta_{t_0}(y_1) + \delta_{t_0}(y_2) + \delta_{t_0}(y_3)) \\
&= A - \delta_{t_0}(y_2) - \delta_{t_0}(y_3) \\
&\le A - 2 \cdot \left\lceil \frac{1}{3}A \right\rceil \\
&\le \frac{1}{3}A,
\end{aligned}$$

这里我们用到 $t_0 \ge \delta_{t_0}(y_1) + \delta_{t_0}(y_2) + \delta_{t_0}(y_3)$（这是成立的，因为在点 t_0 之前，我们始终只对三个通信记录中的至多一个进行篡改），并且在点 t_0 有 $\delta_{t_0}(y_3) \ge \delta_{t_0}(y_2) = \lceil \frac{1}{3}A \rceil$成立。 □

攻击如下所述。

攻击 1

设 x_1，x_2，$x_3 \in \{0,1\}^k$ 是 Alice 可能的三个输入。根据引理 4.2，存在 y_1、$y_2 \in \{x_1, x_2, x_3\}$ 以及通信记录 $T \in \{0,1\}^n$，使得对手在 Alice 的输入为 y_1 和输入为 y_2 两种情况下，都只需篡改至多 $\frac{1}{3}(A_1 + A_2) + 1$ 比特，即可得到通信记录 T。对手只需篡改协议，使最终通信记录为 T。

引理 4.3. 攻击 *1* 成功腐蚀 $\frac{1}{3}A_1 + \frac{1}{3}A_2 + 1$ 比特。

证明。 这直接由引理4.2得出：无论 Alice 拥有 y_1 还是 y_2，对手都能够使 Bob 接收到相同的通信记录，而只需进行 $\frac{1}{3}(A_1 + A_2) + 1$ 比特的篡改。 □

4.2 攻击 2

在我们的第二种攻击中，对手在协议的两个部分中采取不同的行为。在第一部分，对手基本上使 Bob 的反馈看起来是随机的，因此 Alice 最多只能发送一个距离为 $\frac{1}{2}$ 的纠错码。这使得对手可以在第一部分篡改 Alice 的 $\frac{1}{4}$比特，从而使 Bob 无法区分三个输入。随后，在第二部分，我们利用上一部分中的引理 4.2 证明，对手可以只篡改 $\frac{1}{3}A_2$ 比特，就能使 Bob 无法区分剩下三个输入中的两个。

为了论证对手能够在第一节实施攻击，我们需要以下引理。

引理4.4。 对于任意 $0 < \epsilon < 0.1$，假设 *Alice* 有 K 个可能的输入，其中 $K > (4/\epsilon)^{1/3}$。那么，对于任何由 *Alice* 发送 A 比特、*Bob* 发送 B 比特组成的协议，其中 $A + B \ge \log(1/\epsilon)\epsilon^3$，都存在三个输入 x_1, x_2, x_3 以及一份通信记录 T，使得无论 *Alice* 的输入是 x_1, x_2, x_3 中的哪一个，对手最多只需篡改 $\left(\frac{1}{4} + \frac{3\epsilon}{2}\right) \cdot A + \left(\frac{1}{2} + \epsilon\right) \cdot B + 1$ 比特，就能使协议的通信记录变为 T。

证明。令 Λ 表示 Alice 所有可能的 K 输入构成的集合。假设交互式纠错码的轮次安排如下：当 Alice 发送第 t 个比特时，她此前已收到 Bob 发送的 $\gamma(t)$ 比特。对于$b \in \{0,1\}^B$ （b 可以看作 Alice 在整个协议过程中从 Bob 收到的内容），我们定义字符串 $a(y;b)\ a(y_1,y_2,y_3;\ b) \in \{0,1\}^A$ 如下：

- 我们将 $a(y;b)[t]$ 定义为：如果 Alice 的输入是 y，且她目前为止已从 Bob 那里看到 $b[1:\gamma(t)]$，那么这是 Alice 为她的第 t 个比特发送的比特。需要说明的是，这里我们滥用了记号：Alice 的消息 $a(y;b)[t]$ 只取决于 $b[1:\ \gamma(t)]$，而不取决于 b 的其余部分，但为简化记号，我们将 b 全部纳入。

- 对于每个由不同输入 y_1、y_2、y_3 组成的（无序）三元组，我们如下定义 $a(y_1,y_2,y_3;b)[t]$。– 如果 $\max_{i\in\{1,2,3\}} \Delta(a(y_1,y_2,y_3;\ b)[1:\ t-1], a(y_i)[1:\ t-1]) \le \left(\frac{1}{4}+\frac{\epsilon}{2}\right)\cdot A - 1$，则令 $a(y_1,y_2,y_3;b)[t] = \mathrm{maj}(a(y_1;\ b)[t], a(y_2;\ b)[t], a(y_3;\ b)[t])$。– 否则，令 $i \in \{1,2,3\}$ 为满足 $\Delta(a(y_1,y_2,y_3;\ b)[1:\ t-1], a(y_i)[1:\ t-1]) \ge \left(\frac{1}{4}+\frac{\epsilon}{2}\right)\cdot A + 1$ 的值（若 i 有多个取值，则任选其一），并令 $a(y_1,y_2,y_3;\ b)[t] = a(y_i;\ b)[t]$。

命题 *4.5.* 对任意 $b \in \{0,1\}^B$，以及任意三个输入 $y_1,y_2,y_3 \in \Lambda$，若 $\mathrm{Diam}(a(y_1;\ b)\ a(y_2;\ b)\ a(y_3;\ b)) \le \left(\frac{1}{2}+\epsilon\right)\cdot A$，则 $\max_{i\in[3]} \Delta(a(y_1,y_2,y_3;\ b)\ a(y_i;\ b)) \le \left(\frac{1}{4}+\frac{1}{2}\epsilon\right)\cdot A + 1$。

证明。假设 $a(y_1;\ b)\ a(y_2;\ b)\ a(y_3;\ b)$ 满足 $\mathrm{Diam}(a(y_1;\ b)\ a(y_2;\ b)\ a(y_3;\ b)) \le \left(\frac{1}{2}+\epsilon\right)\cdot A$。令 T_{123} 为满足 $t \in [A]$ 的指标，其中 $a(y_1;b)[t] = a(y_2;b)[t] = a(y_3;b)[t]$。再令 T_{12} 为满足 t 的指标，其中 $a(y_1;b)[t] = a(y_2;b)[t] \ne a(y_3;\ b)[t]$，并类似地定义 T_{23} 和 T_{31}。注意，$T_{123}, T_{12}, T_{23}, T_{31}$ 两两不相交，且它们合起来覆盖所有指标 $[A]$。

若 $|T_{12}|, |T_{23}|, T_{31}| < \left(\frac{1}{4}+\frac{\epsilon}{2}\right)\cdot A + 1$，那么注意到，对于所有 $t \in [A]$，$a(y_1,y_2,y_3;\ b)[t] = \mathrm{maj}(a(y_1;\ b)[t], a(y_2;\ b)[t], a(y_3;\ b)[t])$，因此 $\Delta(a(y_1,y_2,y_3;\ b)\ a(y_i;\ b)) = |T_{-i}| \le \left(\frac{1}{4}+\epsilon\right)\cdot A$，其中 T_{-i} 中的 $-i$ 是 $\{1,2,3\}$ 中不等于 i 的另外两个。

否则，$|T_{12}|\ |T_{23}|\ |T_{31}| \left(\frac{1}{4}+\frac{\epsilon}{2}\right)\cdot A |T_{12}|\ |T_{23}| >$ 中至 $\left(\frac{1}{4}+\frac{\epsilon}{2}\right)\cdot A \quad \Delta\ a\ y_1\ b\ \ a\ y_3\ b = |T_{12}| + |T_{23}| > \left(\frac{1}{2}+\epsilon\right)\cdot A$ 多有一个大于，因为例如若，，那么 ((;) (;))，这就产生了矛盾。现在，不失一般性地，假设 $|T_{12}| > \left(\frac{1}{4}+\frac{\epsilon}{2}\right)\cdot A$。在上述设置$a(y_1,y_2,y_3;b)[t]$的算法中，注意我们会一直设置 $a(y_1,y_2,y_3;\ b)[t] = \mathrm{maj}(a(y_1;\ b)[t], a(y_2;\ b)[t], a(y_3;\ b)[t])$，直到第 $\left\lceil\left(\frac{1}{4}+\epsilon\right)\cdot A\right\rceil$ 小的索引 $t_0 \in T_{12}$。之后，我们设置 $a(y_1,y_2,y_3;\ b)[t] = a(y_3;\ b)[t]$。因此，$\Delta(a(y_1,y_2,y_3;\ b)\ a(y_3;\ b)) = \left\lceil\left(\frac{1}{4}+\frac{\epsilon}{2}\right)\cdot A\right\rceil$。注意，对于 T_{12}，还有 $|T_{12}| - \left\lceil\left(\frac{1}{4}+\frac{\epsilon}{2}\right)\cdot A\right\rceil$ 个索引会使 $a(y_1,y_2,y_3;b)[t]$ 被设置为 $a(y_3;\ b)[t]$，而不是 $a(x_1;\ b)[t] = a(x_2;\ b)[t]$。由于对于，，$\left(|T_{12}| - \left\lceil\left(\frac{1}{4}+\frac{\epsilon}{2}\right)\cdot A\right\rceil\right) + |T_{-i}| = |T_{12}| + |T_{-i}| - \left\lceil\left(\frac{1}{4}+\frac{\epsilon}{2}\right)\cdot A\right\rceil \le \left(\frac{1}{2}+\epsilon\right)\cdot A - \left\lceil\left(\frac{1}{4}+\frac{\epsilon}{2}\right)\cdot A\right\rceil \le ( )$，因此对任意 $i = 1\ 2 \quad t \in T_{23}\ \ a\ y_1\ y_2\ y_3\ b\ [t]$ 索引，(, , ;) 都会被设置为$a(y_2;b)[t] = a(y_3;\ b)[t]$；类似地，对任意 $t \in T_{31}$，$a(y_1,y_2,y_3;\ b)[t]$ 都会被设置为 $a(y_3;\ b)[t] = a(y_1;\ b)[t]$。那么，对 $i=1$，$\Delta(a(y_1,y_2,y_3;\ b)\ a(y_i;\ b)) \le \left(\frac{1}{4}+\frac{\epsilon}{2}\right)\cdot A + 1$，2 也成立。 □

现在，我们根据 B 相对于 A 的大小，将引理4.4的证明分为两种情况。若 $B \le \epsilon\cdot(A+B)$，则考虑如下攻击：对手任意选择一个字符串 $b \in \{0,1\}^B$，并篡改 Bob 的通信，使 Alice 收到 b。这至多需要 $B \le \epsilon\cdot(A+B)$ 次篡改。根据推论 3.4，存在三个输入 x_1、x_2、$x_3 \in \Lambda$，使得 $\mathrm{Diam}(a(x_1;\ b)\ a(x_2;\ b)\ a(x_3;\ b)) \le \left(\frac{1}{2}+\epsilon\right)\cdot A$，因此根据命题 4.5，要将 Alice 发往 $a(x_1,x_2,x_3;b)$ 的消息从 $a(x_1;b)\ a(x_2;b)\ a(x_3;b)$ 中任意一个篡改，至多需要 $\left(\frac{1}{4}+\frac{\epsilon}{2}\right)\cdot A + 1$ 次篡改。总计至多需要 $\left(\frac{1}{4}+\frac{3\epsilon}{2}\right)\cdot A + \epsilon B + 1$ 次篡改。

第二种情况是 $B > \epsilon \cdot (A + B)$。在这种情况下，对手选取 (x_1, x_2, x_3) 如下。根据推论 3.4，我们有

$$\Pr_{\substack{(y_1,y_2,y_3)\in\binom{\Lambda}{3}\\ b\in\{0,1\}^B}}\left[\mathrm{Diam}(a(y_1;b),a(y_2;b),a(y_3;b)) \le \left(\frac{1}{2}+\epsilon\right)\cdot A\right] \ge \frac{\epsilon}{4},$$

因此存在 (x_1, x_2, x_3)，使得

$$\Pr_{b\in\{0,1\}^B}\left[\mathrm{Diam}(a(x_1;b),a(x_2;b),a(x_3;b)) \le \left(\frac{1}{2}+\epsilon\right)\cdot A\right] \ge \frac{\epsilon}{4}.$$

特别地，存在一个大小为 $|\Pi| \ge \epsilon \cdot 2^{B-2}$ 的集合 $\Pi \subseteq \{0,1\}^B$，使得对于任意 $b \in \Pi$，都有 $\mathrm{Diam}(a(x_1; b)\ a(x_2; b)\ a(x_3; b)) \le \left(\frac{1}{2}+\epsilon\right)\cdot A$。

现在，考虑如下过程：对于 Bob 的每个比特，对手都以概率 $1/2$ 独立地将其翻转。这定义了一个字符串 $b \in \{0,1\}^B$（在任意时刻，即其前缀）。注意，Alice 收到任意字符串 $b \in \{0,1\}$ 的概率为 2^{-B}，因为 Bob 的每个比特都以 $1/2$ 的概率被翻转。与此同时，对手将 Alice 的比特篡改为 $a(x_1, x_2, \bar{z_3}; b)$（回想一下，$a(x_1, x_2, z_3; b)[t]$ 仅取决于 $b[1: \gamma(t)]$，而不取决于所有 b，因此此攻击定义良好）。

为便于记号表示，令 β 表示 Bob 在整个过程中发送的内容这一随机变量。我们有

$$\begin{aligned}
&\Pr_b\left[\left(\max_{i\in[3]}\Delta(a(x_i;b),a(x_1,x_2,x_3;b)) \le \left(\frac{1}{4}+\frac{\epsilon}{2}\right)\cdot A\right) \wedge \left(\Delta(b,\beta) \le \left(\frac{1}{2}+\epsilon\right)\cdot B\right)\right]\\
&\quad\ge \Pr_b[b\in\Pi] - \Pr_b\left[\Delta(b,\beta) \le \left(\frac{1}{2}+\epsilon\right)\cdot B\right]\\
&\quad\ge \frac{\epsilon}{4} - e^{-2\epsilon^2 B/3}\\
&\quad> \frac{\epsilon}{4} - e^{-2\epsilon^3(A+B)/3},
\end{aligned}$$

其中，第一个不等式源于以下事实：根据命题 4.5，当 $b \in \Pi$ 时，$\le \left(\frac{1}{4}+\frac{\epsilon}{2}\right)\cdot A + 1$ 对 $_{i\in[3]}\ \Delta(a(x_i;\ b)\ a(x_1, x_2, x_3;\ b))$ 成立；第二个不等式由切尔诺夫界推出，最后一个不等式则源于我们的假设 $B > \epsilon \cdot (A + B)$。由于 $\frac{\epsilon}{4} > \epsilon^2 = e^{-2}\log(1/\epsilon) \ge e^{-2\epsilon^3(A+B)/3}$，该表达式为正，因此存在一个 $b \in \{0,1\}^B$ 的取值，使得 $\le \left(\frac{1}{4}+\frac{\epsilon}{2}\right)\cdot A + 1$ 对 $\max_{i\in[3]}\Delta(a(x_i;\ b)\ a(x_1, x_2, x_3;\ b))$ 成立，且 $\Delta(b, \beta) \le \left(\frac{1}{2}+\epsilon\right)\cdot B$。于是，无论 Alice 具有 x_1、x_2 还是 x_3，若对手将 Bob 的消息篡改为 b，并将 Alice 的消息篡改为 $a(x_1, x_2, x_3; b)$，所需的总篡改次数至多为 $\left(\frac{1}{4}+\frac{\epsilon}{2}\right)\cdot A + \left(\frac{1}{2}+\epsilon\right)\cdot B + 1$。

□

现在我们陈述第二种攻击。

攻击 2

设输入 x_1、x_2、$x_3 \in \{0,1\}^k$ 以及通信记录 $T_1 \in \{0,1\}^{21n/47}$ 满足协议第一部分的引理 4.4。那么，对于协议的第一部分，当 Alice 的输入为 x_1、x_2、x_3 时，对手会将通信记录篡改为 T_1，所需的篡改比特数至多为 $\left(\frac{1}{4}+\frac{3\epsilon}{2}\right)A_1 + \left(\frac{1}{2}+\epsilon\right)B_1 + 1$。

对于协议的第二部分，对手按照引理 4.2 中的方法，将通信篡改为通信记录$T_2 \in \{0,1\}^{26n/47}$，使得存在 x_1、x_2、x_3中的两个，记为 y_1、y_2，对手至多可以篡改 $\frac{1}{3}A_2+1$ 的通信，使接收到的比特的通信记录为 T_2，条件是 Alice 的输入为 y_1 或 y_2。

引理 4.6 $k \geq \frac{141 \quad 1/\epsilon}{21\epsilon^3}\cdot$ *2* $\left(\frac{1}{4}+\frac{3\epsilon}{2}\right)\cdot A_1+\left(\frac{1}{2}+\epsilon\right)\cdot$**...**假设 $B_1+\frac{1}{3}A_2+2$ log() 攻击成功篡改了比特。

证明。无论 Alice 是否有 y_1 或 y_2，对手采用此攻击时，Bob 视角下的通信记录看起来都是 T_1 后接 T_2（限制在 Bob 的视角内）。由于$A_1+B_1 \geq \max\{\frac{21}{26}A_2, k-A_2\}$（其中 $A_1+A_2 \geq k$ 成立，因为 Alice 即使在无噪声的情况下，也需要发送 k比特才能传达 x），因此 $A_1+B_1 \geq \frac{21}{47}k \geq 3\log(1/\epsilon)/\epsilon^3$，所以满足引理4.4的条件。于是，根据引理4.4，当 Alice 有 y_1或 y_2时，协议第一部分中使用的篡改次数至多为 $\left(\frac{1}{4}+\frac{3\epsilon}{2}\right)\cdot A_1+\left(\frac{1}{2}+\epsilon\right)\cdot B_1$；根据引理4.2，无论 Alice 有 y_1还是 y_2，第二部分中被篡改的比特数至多为 $\frac{1}{3}A_2+1$。 □

4.3 攻击 3

在我们的第三种攻击中，我们采用以下策略。从整体上看，我们选择两个输入 x_1和 x_2。在协议的第一部分中，Bob 的视图就好像 Alice 拥有 x_1 一样，同时篡改 Bob 的比特，使 Alice 以为他一直在正确接收并作出响应。在协议的第二部分中，随机翻转 Bob 的比特，并篡改 Alice 的通信，使其看起来像是她拥有 x_2。

我们需要的第一个引理是证明：对于协议的第一部分，存在许多输入，使得它们对应的未受篡改的转录之间两两具有较小的汉明距离。

引理 4.7。设 $\epsilon > 0$，并假设 *Alice* 有 K 种可能的输入。那么对于任何由 *Alice* 发送 A 比特、*Bob* 发送 B 比特组成的协议，都存在一个大小为 $K'_\epsilon(K) = K^\epsilon - \frac{1}{\epsilon}$ 的集合 Γ，使得对于任意两个 $x_1, x_2 \in \Gamma$，当 *Alice* 的输入为 x_1 或 x_2 时，未受干扰的通信记录之间的相对距离为 $\leq \left(\frac{1}{2}+\epsilon\right)\cdot(A+B)$。

证明。考虑一个图，其中 K 可能的输入是顶点，并且当 $\Delta(T(x)\ T(y)) \leq \left(\frac{1}{2}+\epsilon\right)\cdot(A+B)$ 时，从 x 向 y 画一条边，其中 $T(z)$ 表示 Alice 的输入为 z 时对应的（未受干扰的）通信记录。根据引理 3.2，不存在大小为$\frac{1}{\epsilon}$ 的独立集。进而，根据定理 3.7，如果不存在一个 $K'_\epsilon(K)$-团，那么 $K < R(K'_\epsilon(K)\frac{1}{\epsilon}) \leq \binom{K'_\epsilon(K)}{1/\epsilon+1/\epsilon} \leq \left(K'_\epsilon(K)+\frac{1}{\epsilon}\right)^{1/\epsilon} = K$，这就产生了矛盾。 □

引理 4.8。令 $\epsilon > 0$，并假设 *Alice* 有 $K' > \sqrt{2/\epsilon}$ 个可能的输入。对于任何由 *Alice* 发送 A 比特、*Bob* 发送 B 比特组成的协议，只要 $A+B > {}^{3}\log(1/\epsilon)\,\epsilon^3$，则存在~~两个输入~~ x_1, x_2，使得对于 *Bob* 在协议开始时收到的任意辅助信息 α（在 *Alice* 和 *Bob* 都确定其策略之后），存在两个通信记录 T_1, T_2，使得 *Bob* 对这两个通信记录的视图相同；并且在 *Alice* 拥有 x_1 的情况下，对手只需篡改 $\left(\frac{1}{2}+2\epsilon\right)A+\left(\frac{1}{2}+\epsilon\right)B$个比特即可得到通信记录 T_1，而在 *Alice* 拥有 x_2 的情况下，对手只需篡改$\left(\frac{1}{2}+\epsilon\right)B$个比特即可使通信记录为 T_2。

证明。令 Λ 为 Alice 的所有可能输入。假设当 Alice 发送第 t 个比特时，她目前已经从 Bob 处看到 $\gamma(t)$ 个比特。对于输入 y 和 $b \in \{0,1\}^B$（b 可以理解为 Alice 在整个协议过程中从 Bob 处接收到的内容），我们定义字符串 $a(y;b)$ 如下：$a(y;b)[t]$ 是 Alice 在输入为 y 且目前已经从 Bob 处看到 $b[1{:}\ \gamma(t)]$ 时所发送的第 t 个比特。我们注意到，Alice 的第 t 个比特只取决于 $b[1:\gamma(t)]$，而不取决于 b 的其余部分；但为便于记号表示，我们将 b 全部包含在内。

如果 Bob 发言 $B \le \epsilon(A+B)$ 比特，则考虑以下攻击：对手选择某个字符串 $b \in \{0,1\}^B$，并篡改 Bob 的比特，使其看起来像 b，最多需要 $B \le \epsilon(A+B)$ 次篡改。设 $a(z;b)$ 为 Alice 在输入 z 并在整个协议过程中收到 b 时所发送的比特。那么，根据推论 3.6，存在两个输入 x_1、x_2，使得 $\Delta(a(x_1;\ b)\ a(x_2;\ b)) < \left(\frac{1}{2}+\epsilon\right)\cdot A$。在 Alice 的两种情况下，对手都可以篡改 Alice 的通信，使其看起来像 $a(x_2;b)$；当 Alice 的输入为 x_1 时，总共需要 $\le \left(\frac{1}{2}+\epsilon\right)\cdot A + \epsilon(A+B)$ $= \left(\frac{1}{2}+2\epsilon\right)\cdot A + \epsilon B$ 次篡改；当 Alice 的输入为 x_2 时，则需要 $\le \epsilon(A+B)$ 次篡改。

<escape>否则，在本证明的余下部分中，假设 Bob 发送 $B > \epsilon(A+B)$ 比特。根据推论 3.6，我们有 </escape>

$$\Pr_{\substack{(y_1,y_2)\in\binom{\Lambda}{2}\\ b\in\{0,1\}^B}}\left[\Delta(a(y_1;b),a(y_2;b)) \le \left(\frac{1}{2}+\epsilon\right)\cdot A\right] \ge \frac{\epsilon}{2},$$

因此存在一个 $(x_1,x_2) \in \binom{\Lambda}{2}$，使得

$$\Pr_{b\in\{0,1\}^B}\left[\Delta(a(x_1;b),a(x_2;b)) \le \left(\frac{1}{2}+\epsilon\right)\cdot A\right] \ge \frac{\epsilon}{2}.$$

特别地，存在一个大小为 $|\Pi| \ge \epsilon\cdot 2^{B-1}$ 的集合 $\Pi \subseteq \{0,1\}^B$，使得对于任意 $b\in\Pi$，都有 $\Delta(a(x_1;\ b)\ a(x_2;\ b)) \le \left(\frac{1}{2}+\epsilon\right)\cdot A$。注意，$(x_1,x_2)$ 的这一选择独立于 Bob 可能收到的任何辅助信息α。

考虑如下过程：对于 Bob 发送的每个比特，我们以$_1$ $_2$的概率将其翻转。这定义了一个字符串 $b \in \{0,1\}^B$（或其前缀）。注意，由于 Bob 的每个比特都以$_1$ $_2$的概率被翻转，Alice 接收到任意字符串$b\in\{0,1\}^B$的概率都是 2^{-B}。与此同时，对手将 Alice 的字符串篡改为 $a(x_2;b)$（注意，$a(x_2;b)[t]$ 仅取决于 $b[1:\ \gamma(t)]$）。 –

在符号表示上，令 β 表示 Bob 在整个过程中发送的内容。我们有

$$\begin{aligned}
&\Pr_b\left[\left(\Delta(a(x_1;b),a(x_2;b)) \le \left(\frac{1}{2}+\epsilon\right)\cdot A\right) \wedge \left(\Delta(b,\beta) \le \left(\frac{1}{2}+\epsilon\right)\cdot B\right)\right]\\
&\quad \ge \Pr_b[b\in\Pi] - \Pr_b\left[\Delta(b,\beta) \le \left(\frac{1}{2}+\epsilon\right)\cdot B\right]\\
&\quad \ge \frac{\epsilon}{2} - e^{-2\epsilon^2 B/3}\\
&\quad \ge \frac{\epsilon}{2} - e^{-2\epsilon^3(A+B)/3}.
\end{aligned}$$

我们有 $\frac{\epsilon}{2} > \epsilon^2 = e^{-2\log(1/\epsilon)} > e^{-2\epsilon^3(A+B)/3}$，因此该表达式为正，故存在一个 $b\in\{0,1\}^B$ 的选择，使得 $\Delta(a(x_1;\ b)\ a(x_2;\ b)) \le \left(\frac{1}{2}+\epsilon\right)\cdot A$，且 $\Delta(b,\beta) \le \left(\frac{1}{2}+\epsilon\right)\cdot B$。换言之，当 Alice 拥有 x_1 时，这次攻击至多使用 $\left(\frac{1}{2}+\epsilon\right)\cdot A + \left(\frac{1}{2}+\epsilon\right)\cdot B$ 次篡改；而当 Alice 拥有 x_2 时，则使用 $\left(\frac{1}{2}+\epsilon\right)\cdot B$ 次篡改。

□

攻击 3

将协议第一部分中 Alice 输入 y 时对应的未受篡改的转录记为 $T_1(y)$。根据引理 4.7，存在一个由 $2^{\epsilon k}-\frac{1}{\epsilon}$ 个输入组成的集合 M，使得对于每个 $y_1, y_2 \in M$，都有 $\Delta(T_1(y_1)\ T_1(y_2)) \leq \left(\frac{1}{2}+\epsilon\right)\cdot n$。接下来，考虑协议第二部分，并假设 Alice 在协议第一部分中看到了 $T_1(x)$（限制在她的视图内）。根据引理 4.8，存在 $x_1, x_2 \in M$，使得无论 Bob 在第二部分开始时收到什么辅助信息 α，都存在转录 $T_{2,}1(\alpha)$ 和 $T_{2,}2(\alpha)$，使得 Bob 对这两份转录的视图相同，并且这两份转录 $T_{2,}1(\alpha) T_{2,}2(\alpha)$ 满足引理 4.8 中列出的性质。

在协议的第一部分，对手篡改通信，使 Bob 始终接收到 $T_1(x_1)$（仅限 Bob 能看到的比特），并使 Alice 接收到 $T(x)$（仅限她能看到的比特），其中 x 表示 Alice 的输入。

在协议的第二部分，对手篡改通信，使通信记录为 $T_{2,\ 1}(\alpha = T_1(x_1))$（当 Alice 的输入为 x_1 时），否则为 $T_{2,\ 2}(\alpha = T_1(x_1))$。

引理 4.9。 假设 $k > {}^{141}\log(1/\epsilon)\ 26\epsilon^3$ 。攻击 *3* 成功篡改

$$\max\left\{\left(\frac{1}{2}+2\epsilon\right)\cdot A_2+\left(\frac{1}{2}+\epsilon\right)\cdot B_2\ ,\quad \left(\frac{1}{2}+\epsilon\right)\cdot A_1+\left(\frac{1}{2}+\epsilon\right)\cdot B_1+\left(\frac{1}{2}+\epsilon\right)\cdot B_2\right\}$$

比特。

证明。无论 Alice 的输入为 x_1 还是 x_2，Bob 收到的通信记录（仅限他的视图）都相同。由于 $A_2+B_2 \geq \max\{\frac{26}{21}A_1, k-A_1\}$（其中 $A_1+A_2 \geq k$ 成立，因为即使没有噪声，Alice 也需要发送 k 比特来传达 x），因此 $A_2+B_2 \geq \frac{26}{47}k > {}^{3}\log(1/\epsilon)\ \epsilon^3$，所以引理 4.8 的条件得到满足。如果 Alice 的输入为 x_1，第一部分的篡改量为 0，而第二部分中对手最多篡改 $\left(\frac{1}{2}+2\epsilon\right)A_2+\left(\frac{1}{2}+\epsilon\right)\cdot B_2$ 比特。如果 Alice 的输入为 x_2，第一部分的篡改量为 $\Delta(T_1(x_1)\ T_1(x_2)) \leq \left(\frac{1}{2}+\epsilon\right)\cdot(A_1+B_1)$，而第二部分中对手最多篡改 $\left(\frac{1}{2}+\epsilon\right)\cdot B_2$ 比特。 □

4.4 定理4.1的证明

本节将证明我们的主要定理，下面重新陈述该定理。

定理 4.1。 对于足够小的 $\epsilon > 0$，那么对于所有 $k > 100\epsilon^{-4}$，没有任何针对 $x \in \{0,1\}^k$ 的交互式纠错码能够以大于$_{1\ 2}$的概率抵御超过 $\frac{13}{47}+2\epsilon$ 比例的错误。

我们先从以下引理开始。

引理 4.10. 对于任意非负的 a_1，b_1，a_2，$b_2 \in \mathbb{R}$，其中 $a_1+b_1 = \frac{21}{47}$ 且 $a_1+b_1+a_2+b_2 = 1$，定义

$$\begin{aligned}\delta_1 &= \frac{1}{3}a_1+\frac{1}{3}a_2,\\ \delta_2 &= \frac{1}{4}a_1+\frac{1}{2}b_1+\frac{1}{3}a_2,\\ \delta_3 &= \max\left\{\frac{1}{2}a_2+\frac{1}{2}b_2, \frac{1}{2}a_1+\frac{1}{2}b_1+\frac{1}{2}b_2\right\}.\end{aligned}$$

有

$$\min\{\delta_1, \delta_2, \delta_3\} \le \frac{13}{47}.$$

证明。 利用 $b_1 = \frac{21}{47} - a_1$ 和 $b_2 = \frac{26}{47} - a_2$，我们可以代入：

$$\begin{aligned}
\delta_1 &= \frac{1}{3}a_1 + \frac{1}{3}a_2, \\
\delta_2 &= \frac{21}{94} - \frac{1}{4}a_1 + \frac{1}{3}a_2, \\
\delta_3 &= \max\left\{\frac{13}{37}, \frac{1}{2} - \frac{1}{2}a_2\right\}.
\end{aligned}$$

然后，

$$\min\{\delta_1, \delta_2, \delta_3\} \le \frac{13}{47} \iff \min\{\delta_1, \delta_2, \delta_3'\} \le \frac{13}{47},$$

其中 $\delta_3' = \frac{1}{2} - \frac{1}{2}a_2$。但请注意，

$$\frac{9}{35}\delta_1 + \frac{12}{35}\delta_2 + \frac{2}{5}\delta_3' = \frac{13}{47}$$

其中 权重 $\frac{9}{35}$、$\frac{12}{35}$、$\frac{2}{5}$之和为 1，因此 δ_1、δ_2、δ_3' 中至少有一个必须至多为 $\frac{13}{47}$。□

定理 *4.1*的证明。 回顾一下，交互式纠错码 的长度为 $n := A_1 + B_1 + A_2 + B_2 \ge A_1 + A_2 \ge k > \epsilon^{-3}$（因为 Alice 至少需要发送 k 比特来传达 x，即使在无噪声设置下也是如此）。我们的目标是证明，无论 A_1、B_1、A_2、B_2的值如何，攻击 1、2和 3中至少有一种所需的 $\left(\frac{13}{47} + 2\epsilon\right) \cdot n$ 篡改次数至多为。

根据引理4.3，攻击1成功使用

$$\frac{1}{3}A_1 + \frac{1}{3}A_2 + 1 \le (\delta_1 + 2\epsilon)\, n$$

比特进行篡改，其中 $\delta_1 := (\frac{1}{3}A_1 + \frac{1}{3}A_2)/n$。

根据引理4.6，攻击2成功使用

$$\left(\frac{1}{4} + \frac{3\epsilon}{2}\right) \cdot A_1 + \left(\frac{1}{2} + \epsilon\right) \cdot B_1 + \frac{1}{3}A_2 + 2 \le \frac{1}{4}A_1 + \frac{1}{2}B_1 + \frac{1}{3}A_2 + 2\epsilon n = (\delta_2 + 2\epsilon)n$$

比特进行篡改，其中我们定义 $\delta_2 = (\frac{1}{4}A_1 + \frac{1}{2}B_1 + \frac{1}{3}A_2)/n$。B

y L 4 9 Attack 3 成功 ds using

艾玛。，

$$\begin{aligned}
&\max\left\{\left(\frac{1}{2} + 2\epsilon\right) \cdot A_2 + \left(\frac{1}{2} + \epsilon\right) \cdot B_2\ ,\quad \left(\frac{1}{2} + \epsilon\right) \cdot A_1 + \left(\frac{1}{2} + \epsilon\right) \cdot B_1 + \left(\frac{1}{2} + \epsilon\right) \cdot B_2\right\} \\
&\quad \le \max\left\{\frac{1}{2}A_2 + \frac{1}{2}B_2 + 2\epsilon n, \frac{1}{2}A_1 + \frac{1}{2}B_1 + \frac{1}{2}B_2 + 2\epsilon n\right\} \\
&\quad = (\delta_3 + 2\epsilon)n
\end{aligned}$$

篡改比特，其中我们定义 $\delta_3 =$最大值 $\{\frac{1}{2}A_2 + \frac{1}{2}B_2, \frac{1}{2}A_1 + \frac{1}{2}B_1 + \frac{1}{2}B_2\}$ / n.

根据引理 4.10，我们有 $\min\{\delta_1, \delta_2, \delta_3\} \le \frac{13}{47}$，因此无论 $\left(\frac{13}{47} + 2\epsilon\right) \cdot n$ 的相对比例如何，三种攻击中至少有一种能以 A_1 篡改成功，B_1、A_2、B_2。

□

参考文献

[ADL06] Rudolf Ahlswede、Christian Deppe 和 Vladimir Lebedev。具有无噪声反馈、局部化错误或两者兼有的非二元纠错码。载于2006年IEEE国际信息论研讨会，页2486–2487，2006年。2、3[BEK+22] Mark Braverman、Klim Efremenko、Gillat Kol、Raghuvansh Saxena 和 Zhijun Zhang。二元反馈信道中轮数与抗扰性的权衡。计算复杂性电子讨论会，TR22-179，2022年12月。3[Ber64] Elwyn R. Berlekamp。具有无噪声反馈的分组编码。1964年。1、2、5[Ber68] Elwyn R. Berlekamp。具有无噪声、无延迟反馈的二元对称信道分组编码。纠错码，页61–88，1968年。2[BY08a] Marat Burnashev 和 Hirosuke Yamamoto。关于具有有噪声反馈的BSC的零速率错误指数。信息传输问题，44，2008年9月。3[BY08b] Marat V. Burnashev 和 Hirosuke Yamamoto。关于BSC、有噪声反馈和三条消息。载于2008年IEEE国际信息论研讨会，页886–889，2008年。3[EKSZ22] Klim Efremenko、Gillat Kol、Raghuvansh Saxena 和 Zhijun Zhang。通过交互实现抗扰能力超过1/4的二元码。IEEE计算机科学基础年会论文集，FOCS，2022年。1、2[GGZ22] Meghal Gupta、Venkatesan Guruswami 和 Rachel Yun Zhang。具有最少无噪声反馈的二元纠错码。即将发表于2023年STOC，2022年。2[GKZ22] Meghal Gupta、Yael Tauman Kalai 和 Rachel Yun Zhang。可抵御 $> 1/2$ 对抗性破坏的二元擦除信道交互式纠错码。载于第54届ACM SIGACT计算理论年会论文集，页609–622，2022年。1、2[GZ22] Meghal Gupta 和 Rachel Yun Zhang。可抵御 $1/2$ 对抗性擦除的正速率二元交互式纠错码。arXiv预印本 arXiv:2201.11929，2022年。2[Ham50] R. W. Hamming。检错码与纠错码。贝尔系统技术期刊，29(2):147–160，1950年。1[HKV15] Bernhard Haeupler、Pritish Kamath 和 Ameya Velingker。部分无噪声反馈通信。载于APPROX-RANDOM，2015年。2[Ram87] Frank P Ramsey。形式逻辑中的一个问题。组合学经典论文，页1–24，1987年。4[Sha48] Claude E. Shannon。通信的数学理论。贝尔系统技术期刊，27(3):379–423，1948年。1[She83] James B. Shearer。关于无三角形图独立数的一则注记。离散数学，46(1):83–87，1983年1月。4

[SW92] Joel Spencer 和 Peter Winkler。说谎者的三个阈值。组合学、概率与计算，1(1):81–93，1992。2[Tur41] Paul Turán。图论中的一个极值问题。*Matematikai és Fizikai Lapok*，48:436–452，1941。4[WQC17] Gang Wang、Yanyuan Qin 和 Chengjuan Chang。部分含噪反馈通信。载于*2017 IEEE*计算机与通信研讨会 *(ISCC)*，第602–607页，2017年。3[Zig76] K.Sh. Zigangirov。通过带反馈的二元对称信道传输时的可纠正错误数。信息传输问题，12:85–97，1976年。2