带反馈信道中纠正一个错误

Ilya Vorobyev、Alexey Lebedev、Vladimir Lebedev、Christian Deppe

arXiv:2301.01848v1 [cs.IT] 4 Jan 2023

摘要

我们研究如何在具有无错误即时反馈的任意离散无记忆信道中纠正单个错误。针对一次反馈的情况，我们提出了一种构造最优传输策略的方法。所得结果使我们能够证明，对于二元信道，两次反馈足以传输与完全反馈情况下相同数量的消息。我们还将所开发的技术应用于二元非对称信道，为较短长度构造传输策略。

I. 引言

我们研究在具有无差错即时反馈的任意离散无记忆信道中纠正单个错误的问题。下文中，我们始终假设所有这些条件——信道无记忆且具有无差错即时反馈——均得到满足。我们主要关注二元对称信道和非对称信道。在二元对称信道中，任何符号都可能被错误地传输，例如用 0 代替 1，反之亦然。通常省略“对称”一词，这种信道简称为二元信道。在二元非对称信道中，发送符号 1 时可能收到 0，但符号 0 总是无误地传输。我们考虑这种带反馈信道的组合模型，其中存在单个传输错误。

众所周知，在具有完全反馈的二元信道中纠正 t 个错误的问题，等价于以下组合搜索问题：需要通过 n 个如下类型的问题找到元素 $x \in \mathcal{M}$：“元素 x 是否属于集合 A，而该集合是集合 $\mathcal{M}$ 的子集？”问题依次提出，即每个后续问题都可以根据先前问题的答案来确定。回答问题的对手知道 x，并且最多可以说谎 t 次。这个问题最初由 R´enyi [1] 提出。对于具有完全反馈的二元信道中线性数量的错误，Berlekamp [2] 和 Zigangirov [3] 计算出了最优传输率。Ulam 在其传记 [4] 中提出了一个类似的、针对 $M = 10^6$ 的问题，此后这个问题广为人知。针对所有M 的最优策略已分别在 [5] 中针对 $t = 1$、在 [6] 中针对 $t = 2$，以及在 [7] 中针对 $t = 3$ 得出。文献 [8] 展示了不同 t 和 $M \leq 2^{20}$ 取值下的最优策略表。

在具有完全反馈的二元非对称信道中进行错误纠正，等价于带半说谎的乌拉姆问题的一个变体，该问题最早在 [9] 中描述。与原始问题的区别在于，只有当真实答案为肯定时才允许说谎。关于这一问题的研究成果综述可见 [10]。对于固定数量 t 的错误，$\mathcal{M}$ 的最大基数渐近等价于 $2^{n+t}/\binom{n}{t}$。对于 $t = 1$，这一结论在 [11]，中得到证明；对于任意 t，则见 [12], [13]。

请注意，对于固定数量的错误，即使只有一次反馈，也足以渐近地传输与完全反馈情形相同数量的消息。对于非二元对称信道，这一结论在 [14]，中得到证明；对于任意离散信道，则见 [15]。

本文的一个重要结果是描述了任意离散信道中采用一次反馈并纠正单个错误的最优策略。我们将所提出的技术应用于构造具有一次或两次反馈的二元信道单个错误纠正传输策略，也用于构造具有一次反馈的二元非对称信道单个错误纠正策略。我们认为，所得结果中最有趣的是构造了一种具有两次反馈的策略

Ilya Vorobyev 和 Christian Deppe 任职于德国慕尼黑慕尼黑工业大学通信工程研究所。（电子邮件：ilya.vorobyev@tum.ru，christian.deppe@tum.de）Alexey Lebedev 和 Vladimir Lebedev 任职于俄罗斯莫斯科哈尔克维奇信息传输问题研究所。（电子邮件：al lebed95@mail.ru，lebedev37@mail.ru）

该策略能够纠正二元信道中的单个错误，并传输与完全自适应策略同样多的消息。

本文其余部分安排如下。第二节给出基本定义。第三节提出并证明一个定理，描述存在单个错误和一次反馈时最优策略的结构。第四节将主要定理应用于构造二元信道中的单错纠正传输策略，该策略具有两次反馈，并且能够传输与完全反馈情形下同样多的消息。最后一节将所提出的技术应用于寻找二元非对称信道中存在单个错误和一次反馈时的良好策略。

II. 基本定义

考虑一个输入字母表为 $\mathcal{X} = \{0, \ldots, q-1\}$、输出字母表为 $\mathcal{Y} = \mathcal{X}$的 q元信道。编码器发送消息$\mathbf{x} \in \mathcal{X}^n$，解码器接收消息$\mathbf{y} \in \mathcal{Y}^n$。向量$\mathbf{y}$的长度为$p$ 的前缀记作$\mathbf{y}^p$。所谓错误，是指将序列$\mathbf{x}$中的一个符号 q_1 替换为符号 q_2 $q_1 \neq q_2$。我们定义一个二部图 G，其左侧对应于$\mathcal{X}$中的元素，右侧对应于 $\mathcal{Y}$中的元素。如果错误可能将符号 q_1 变为 q_2，则在 $q_1 \in \mathcal{X}$和 $q_2 \in \mathcal{Y}$ $q_1 \neq q_2$之间连一条边。图1给出了单向三元信道对应的此类图的示例。

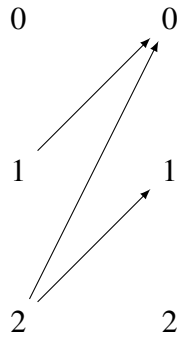

图 1. 单向三元信道的错误图。

本文考虑在具有 k 反馈的信道上进行传输。设码字长度 n 分为 $k+1$ 部分：

$$n = n_1 + n_2 + \ldots + n_{k+1}.$$

编码器发送消息 $m \in [M]$。最初发送的 n_1 个符号 $x_1, \ldots, x_{n_1}$ 仅取决于消息 m。发送完 N_{i-1}：$= n_1 + \ldots + n_{i-1}$, $i \geq 2$ 个符号后，编码器从反馈信道获得接收符号 $\mathbf{y}^{N_{i-1}}$的值。编码器发送第 i 个由 n_i 个符号组成的码块，该码块是消息 m 以及编码器接收到的符号 $\mathbf{y}^{N_{i-1}}$的函数。当$k = 0$ 时，对应于无反馈信道；当 $k = n - 1$时，则对应于具有完全反馈的信道。

我们将消息 m 的云 $B_t(m)$（当 $t = 1$时也记作 $B(m)$）定义为：在传输该消息期间，信道输出中至多出现 t 个错误时可能得到的序列 $\mathbf{y}$ 的集合。我们将互不相交的云 $B_t(m)$, $m \in [M]$的集合称为可纠正 t个错误的码 $\mathcal{C}$。不属于任何云的空间点称为自由点，记作 $\mathcal{F}(\mathcal{C})$。不使用反馈的码称为非自适应码。

注意，对于没有反馈的对称信道，云是汉明度量下半径为 t 的球。对于对称信道，所有云的大小都相同，但对于任意错误图则不然。对于本文提出的构造，寻找在每种长度和每种基数下具有最大自由点数的码是有意义的。这类码称为 F-最优码。

例如，我们来描述具有单个错误和完全反馈的二元信道中云的结构。每个云 $B(m)$ 都包含一个序列 y；如果信道中没有错误，该序列就会被传输。我们称它为根序列。对于任意坐标 i，云中都包含一个序列 y(i)，它在前 $i-1$ 个位置上与 y 相同，在第 i 个位置上与之不同，而在其他所有位置上的符号则任意。因此可见，每个云至少由 $n+1$ 个序列组成。特别地，这给出了最大传输消息数的汉明界。

III. 一次反馈

本节针对单个错误和一次反馈的情形，提出一种传输策略。我们将码字长度 n 分为两部分：n_1 和 n_2，其中 $n = n_1 + n_2$。我们定义一个二部图 $H = (U \sqcup V, E)$ 如下。左右两部分分别由 q^{n_1} 个顶点组成，对应于输入序列集和输出序列集。如果与 v 对应的序列可以由与 u 对应的序列经过单个错误得到，则顶点 u 和 v 之间连一条边。注意，我们不连接对应于相同序列的顶点（这对应于没有错误的情形）。

定理 1. 给定图 $H = (U \sqcup V, E)$。存在一种能够传输

$$M = \sum_{u \in U} M(u) \tag{1}$$

消息的策略，当且仅当存在一族长度为 n_2、基数为 $M(u)$ 且含有 $F(u)$ 个自由点的单错误纠正码 $C(u)$，并满足条件

$$\sum_{u:\,(u,v)\in E} M(u) \le F(v) \tag{2}$$

对于任意 $v \in V$。

证明。下面描述一种任意的编码策略。首先，传输一个长度为 n_1 的序列 u，它对应于图 H 左侧部分 U 中的一个顶点 u。设以序列 u 开头的消息数量为 $M(u)$。考虑前 n_1 个符号没有发生错误的情况。对于剩余的 n_2 个符号，我们需要传输 $M(u)$ 条不同的消息，且可能发生一个错误。因此，我们需要使用长度为 n_2、基数为 $M(u)$ 的单错误纠正码 $\mathcal{C}(u)$。用 $F(u)$ 表示 $C(u)$ 的自由点数量。

如果前 n_1 个符号中发生了错误，且接收到的不是 u，而是序列 v，那么为了传输以 u 开头的 $M(u)$ 条消息，我们需要 $M(u)$ 个点，这些点必须是 $\mathcal{C}(v)$ 的自由点。

因此，对于每条消息 v，都应存在一个码 $\mathcal{C}(v)$，其自由点分布在所有能够到达序列 v 的序列 u 中；并且每个这样的序列 u 至少必须获得 $M(u)$ 个自由点。当且仅当条件 (2) 成立时，这才有可能。

现在我们描述解码算法。设前 n_1 个接收符号组成的序列对应顶点 $v \in V$；用 a 表示最后 n_2 个符号组成的序列。若 a 不是 $\mathcal{C}(v)$ 中的自由点，这意味着消息的第二部分发生了错误。此时，消息的第二部分对应于 a 所属球的球心。

若序列 a 是 $\mathcal{C}(v)$ 中的自由点，那么它对应于某个序列 u，由该序列可以得到 v。于是，恰好就是这个序列 u 在第一次编码阶段被传输了。根据在至少 $M(u)$ 个与 u 对应的点中使用了哪一个点 a，即可恢复消息的第二部分。 □

我们不知道有什么高效的方法（关于码长为多项式时间）可以找到满足 (2) 的最优码族。不过，即使对所有序列 $u \in \mathcal{X}^{n_1}$ 都选择相同的码，也能取得良好效果，如推论1所示。

举例说明在二元信道中选择相同的码并非最优，请考虑 $n_1 = 2$ 和 $n_2 = 1$ 的情况。选择相同的码时，消息的最大数量为

总是能被 2^{n_1} 整除，而在此情况下结果为 0，因为即使采用自适应方式，长度为 3 时最多也只能传输两条消息。如果选择两个不同的码，则可以传输两条消息。

下面将用二元对称信道的以下结论来构造具有两次反馈的最优策略。

推论1。设 $n_2 = 2^k - 1$, $n_1 = n - n_2$, $k \geq 1$。那么，在存在单个错误且具有一次反馈的对称信道中，我们可以传输

$$M_1(n) = 2^{n_1} \left\lfloor \frac{2^{n_2}}{n_1 + n_2 + 1} \right\rfloor$$

条消息。

证明。对每个点 u，将长度为 n_2 、删去 x 个码字的汉明码指定为 $\mathcal{C}(u)$。我们选择 x ，使其满足约束 (2)。这等价于不等式

$$x2^k \geq n_1(2^{n_2-k} - x),$$

由此可得

$$x \geq \frac{n_1 2^{n_2-k}}{n_1 + 2^k}.$$

于是我们可以取 $x = \left\lceil \frac{n_1 2^{n_2-k}}{n_1+2^k} \right\rceil$。所选码中剩余字的数量为

$$2^{n_2-k} - \left\lceil \frac{n_1 2^{n_2-k}}{n_1 + 2^k} \right\rceil = \left\lfloor \frac{2^{n_2}}{n_1 + 2^k} \right\rfloor = \left\lfloor \frac{2^{n_2}}{n_1 + n_2 + 1} \right\rfloor$$

传输消息的总数为

$$M_1(n) = 2^{n_1} \left\lfloor \frac{2^{n_2}}{n_1 + n_2 + 1} \right\rfloor.$$

□

IV. 带反馈的二元对称信道

用 $Alg_k(n)$ 表示一个长度为 n 、包含一个错误并有 k 次反馈的信道中的传输策略。现在我们描述一种算法：给定 $Alg_{k-1}(n-1)$，构造策略 $Alg_k(n)$，该策略将在下文中使用。

给定 $Alg_{k-1}(n-1)$，用 DADA（加倍与删除算法）算法构造策略 $Alg_k(n)$。

回想一下，在长度为 $n-1$ 的二元对称信道中，每个云都包含一个根消息，以及 $n-1$ 个附加消息；这些消息的前 $i-1$ 个符号与根消息相同，而第 i 个符号与之不同，其中 $i = 1$、2、.....、$n-1$。对于每个长度为 $n-1$ 的消息云，我们通过在每条消息前添加前缀 0 和 1，分别构造两组长度为 n 的消息。要从第一组（第二组）构造长度为 n 的云，只需添加任意一条以 1（0）开头的消息。我们将这类集合称为不完整云。接下来，对于每个自由点，我们通过添加前缀 0 或 1，将其变为两个自由点。我们用尽所有可用的空闲序列，将若干不完整云转化为云。如果不完整云的数量不超过长度为 n 的空闲序列数量，那么经过这一过程后，我们将得到 $2M(n-1)$ 个云和若干自由点，其中 $M(n-1)$ 是通过 $Alg_{k-1}(n-1)$ 算法传输的消息数量。在这种情况下，DADA 算法即告完成。

否则，到这个过程结束时，我们将有若干个云和若干个不完整云，它们将完全覆盖整个空间。

之后，我们会选取一个以 1 开头的不完整序列云和一个以 0 开头的不完整序列云，并将它们的所有元素转换为自由点，从而消除这两个云。这一

操作会产生 $2n$ 个自由点。然后，利用自由点将不完整云转换为云。重复这一操作，直到不完整云全部消除。

过程结束时，剩下偶数个云以及至多 $2n$ 个自由点。如果自由点的数量为 $2n$，这意味着这些自由点刚刚由两个不完整云生成。于是，我们将其中一个不完整云还原，并添加一个自由点，将其变为一个云。这样，我们就得到一个额外的云。

因此，我们证明了以下定理。

定理 2. 假设在长度为 $n-1$ 时，我们已构造出 $M(n-1)$ 个云，用于传输具有单个错误和 $k-1$ 个反馈的消息，$k=1,\dots,n-1$。令

$$U(n)=2\left\lfloor\frac{2^n}{2(n+1)}\right\rfloor,\qquad r(n)=2^n-(n+1)U(n).$$

那么，DADA 算法构造出一个策略 $Alg_k(n)$，用于传输 $M(n)$ 条消息，其中

$$M(n)=\begin{cases}2M(n-1) & \textit{if } 2M(n-1)\le\frac{2^n}{n+1},\\ U(n) & \textit{if } 2M(n-1)>\frac{2^n}{n+1} \textit{ and } r(n)<2n,\\ U(n)+1 & \textit{if } 2M(n-1)>\frac{2^n}{n+1} \textit{ and } r(n)\ge 2n.\end{cases}$$

在完全反馈情形下，已计算出能够在出现单个错误时传输的消息数的最大值，见 [5]。在定理 3 中，我们将给出这一结果的一种更简洁的新证明。

定理 3. 设

$$U(n)=2\left\lfloor\frac{2^n}{2(n+1)}\right\rfloor,\qquad r(n)=2^n-(n+1)U(n).$$

那么，一个 可以通过存在一个单个错误的信道传输 $M_{\mathrm{ad}}(n)$条消息，其中

$$M_{\mathrm{ad}}(n)=\begin{cases}U(n) & \textit{if } r(n)<2n,\\ U(n)+1 & \textit{if } r(n)\ge 2n.\end{cases}\tag{3}$$

此外，这个消息数是最优的。

注 1. 事实上，r 总是偶数，且小于 $2n+2$；因此，式 (3) 最后一行中的条件 $r\ge 2n$ 可以替换为 $r=2n$。注意，第二种情况极少出现。具体而言，对于 $n=1$、2，码基数为 $U(n)+1$，而下一个出现这种情况的长度是 49 736。因此，最优消息数通常是汉明界不超过的最大偶数。

证明. 我们将归纳地构造一种传输策略。对于 $n\le 8$，这个公式可以通过手算验证。

现在假设对于长度为 $n-1$、$n\ge 9$ 的情形，我们已构造出 $M_{\mathrm{ad}}(n-1)$ 个云。注意，不完整云的数量至少为

$$2M_{\mathrm{ad}}(n-1)\ge\frac{2^n}{n}-4>\frac{2^n}{n+1}$$

对于 $n\ge 9$。我们使用 DADA 算法，根据长度为 $n-1$ 的策略构造长度为 n 的自适应策略。由于

$$2M_{\mathrm{ad}}(n-1)>\frac{2^n}{n+1},$$

我们得出，$M_{\mathrm{ad}}(n)$ 等于 $U(n)$ 或 $U(n)$，具体取决于 $r(n)$，正如所需。 □

定理 4. 在具有两次反馈和单个错误的二元信道中，可以传输 $M_{\mathrm{ad}}(n)$条消息，即与采用完全反馈进行传输时的数量相同。

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16
M_1	2	2	4	8	16	28	50	90	168	312	580	1088	2048	3854
M_{ad}	2	2	4	8	16	28	50	92	170	314	584	1092	2048	3854

表 I 单个错误下二元对称信道中可传输消息的最大数量：采用一次反馈和完全反馈时。

请注意，一次反馈不足以实现这一点，这可从表 I 中看出。

证明。我们使用 DADA 算法，根据 $Alg_1(n-1)$ 构造 $Alg_2(n)$。对于 $Alg_1(n-1)$，我们采用推论1中构造的策略，其中

$$M_1(n-1) = \left\lfloor \frac{2^{n_2}}{n_1+n_2+1} \right\rfloor 2^{n_1},$$

其中 $n_2 = 2^k - 1$ 和 $n_1 = n-1-n_2$。

注意（见表 I），对于 $n \le 9$，即使只有一次反馈，也足以传输与采用完全反馈进行编码时相同数量的消息。因此，只需证明关于 $n \ge 10$ 的陈述。我们来证明

$$2M_1(n-1) > \frac{2^n}{n+1}$$

对于 $n \ge 10$。

这等价于不等式

$$2^{n_1+1} \left\lfloor \frac{2^{n_2}}{n_1+n_2+1} \right\rfloor > \frac{2^{n_1+n_2+1}}{n_1+n_2+2}.$$

化简 2^{n_1+1} 并利用不等式 $\lfloor x \rfloor > x-1$，可得

$$\left\lfloor \frac{2^{n_2}}{n_1+n_2+1} \right\rfloor > \frac{2^{n_2}}{n_1+n_2+1} - 1 \ge \frac{2^{n_2}}{n_1+n_2+2}.$$

后一个不等式等价于

$$2^{n_2} \ge (n_1+n_2+1)(n_1+n_2+2).$$

回想一下 $n_2 \ge n_1$ 和 $n_2 = 2^k - 1$，我们得出该不等式在 $n_2 \ge 15$时成立 .

因此，我们证明了不等式 $2M_1(n-1) > \frac{2^n}{n+1}$ 在 $n \ge 16$时成立。对于 $n \in [10, 15]$，可利用表 I 手工验证该不等式。应用定理 2 和定理 3，即可得到所需结果。 □

V. 二元非对称信道

本节将上述定理应用于二元非对称信道。为此，我们需要编制含有许多自由点的码表。为了找到这样的码，我们采用线性规划方法。

在 [16]–[18]，中，线性规划被用于证明纠正非对称错误的非自适应码基数的上界。我们对那些论文中的方法加以改进，从而得到固定长度和基数的码中自由点数量的上界。

记 $M_Z(n,t)$ 为长度为 n、可纠正 t 个错误的非对称码的最大基数。此外，记 $L(n,d,w)$ 和 $U(n,d,w)$ 分别为重量为 w、长度为 n、距离为 d 的恒重码基数的下界和上界。

定理5。设 $n \ge 2t \ge 2$, $1 \le M \le M_Z(n,t)$。定义

$$\overline{F}(n,M,t) = \max\left(2^n - \sum_{i=0}^{n}\left(z_i \sum_{j=0}^{t}\binom{i}{i-j}\right)\right),$$

其中，最大值取遍所有满足以下条件的 z_i：

1) z_i *are nonnegative integers;*
2) $z_0 = 1,\ z_1 = z_2 = \ldots = z_t = 0$*;*
3) $\sum_{i=1}^{s} \binom{n-w+i}{i} z_{w-i} + \sum_{j=0}^{t-s} \binom{w+j}{j} z_{w+j} \le \binom{n}{w}$ *for* $0 \le s \le t < w < n-t$*;*
4) $\sum_{j=s}^{r} z_j L(r-s, 2t+2, r-j) \le U(n+r-s, 2t+2, r)$ *for* $0 \le s \le r$*;*
5) $\sum_{j=s}^{r} z_{n-j} L(r-s, 2t+2, r-j) \le U(n+r-s, 2t+2, r)$ *for* $0 \le s \le r$*;*
6) $\sum_{i=1}^{s} \binom{n-w+i}{i} z_{w-i} + \sum_{j=0}^{t-s} \binom{w+j}{j} z_{w+j} + \left(\binom{w+t-s+1}{w} - \binom{t+1}{t-s+1} \left\lfloor \frac{w+t-s+1}{t+1} \right\rfloor \right) \times z_{w+t-s+1} \le \binom{n}{w}$ *for* $0 \le s \le t < w < n-t$*,*

   $\sum_{i=1}^{s} \binom{n-w+i}{i} z_{w-i} + \sum_{j=0}^{t-s} \binom{w+j}{j} z_{w+j} + \left(\binom{n-w+s+1}{s+1} - \binom{t+1}{t-s} \left\lfloor \frac{n-w+s+1}{t+1} \right\rfloor \right) \times z_{w-s-1} \le \binom{n}{w}$ *for* $0 \le s \le t < w < n-t$*;*
7) $\sum_{i=0}^{n} z_i = M.$

那么，码长为 n、码基数为 M 且可纠正 t 个非对称错误的码中，自由点的数量 F 不大于 $\overline{F}(n, M, t)$。

证明。用 z_i、 $0 \le i \le n$表示码长为 n 且可纠正 t个非对称错误的码中重量为 i 的码字数量。在 [16]–[18] 中，已证明 z_i 必须满足条件1和3–6。显然，自由点数量最多的码必须满足条件2。最后一个条件确定了所考虑码的码基数。最大化的表达式$\overline{F}(n, M, t)$对应于重量分布为 $\{z_i\}$的码中的自由点数量。 □

我们还采用线性规划方法来寻找自由点数量最多的码。固定码长 n、码基数 M以及可纠正的非对称错误数量 t 。引入 2^n个二元变量 x_i ，分别对应所有可能的码字。对于每个点 p，定义集合 $D_t(p)$，其中包含经 t 个非对称错误后可以到达该点的码字。施加约束$\sum_{i \in D_t(p)} x_i \le 1$。对于 $t = 1$，我们将最大化自由点的数量 $2^n - \sum_{i=0} z_i(i+1)$，其中 z_i 是 i 重量为 i 的码字数量。注意，自由点的数量可以用变量 x_i 表示。加入约束 $\sum x_i = M$ 以固定码基数。注意，线性规划问题的任何解（如果存在）都会给出在码长和码基数固定时自由点数量的最优值。为加快计算，我们加入了定理5中的约束。

尽管进行了这些优化，该程序仍有 2^n 个变量，因此只有在 n 的值足够小时才能找到解。表 II 列出了 $t = 1$、 $n = 6$、 7、 8 和 9 对应的一些 F 最优码的参数。最优重量分布见表 III。

长度为 $n = 6$、8 和 9 的码的参数与定理5给出的上界一致。对于 $n = 7$ 和 $M = 18$，我们得到 48 个自由点，而定理5给出的上界为 49 个；也就是说，定理5的上界未能达到。其他所有取值均与上界一致。

长度为 $n = 7$ 和 8 时，具有最优重量分布的码已在 [16]中构造出来。长度为 $n = 6$ 的码此前也已为人所知。对于长度为 $n = 6$ 和 8 以及所有基数 $M \le M_Z(n, 1)$,

可以通过从表 III 中给出重量分布的最大基数码中删除 $M_Z(n,d)$ 个最大重量码字，得到最优码。对于长度为 $n=7$、基数为 $M=17$的情况，我们已知两种重量分布不同且自由点数达到最优的码：$1+0+3+5+5+3+0+0$ 和 $1+0+3+5+6+1+1+0$。从具有第二种重量分布的码中删除最大重量码字，可以得到所有 $M<17$的 F-最优码。不过，只有具有第一种重量分布的码才能扩充为基数为 18 的码。

该程序适用于所有 $n<9$。对于更大的长度，计算复杂度过高。由于长度为 $n=6$ 和 8 的 F最优构造是嵌套码，对于长度为 $n=9$ 的情况，我们也将搜索范围限制在这类码族中。借助这一方法，我们找到了一族嵌套码，其中最大基数为 62 的码具有表 III 所示的重量分布。该码族中各个基数为 M的码的自由点数量都达到了定理5给出的上界。这意味着所构造码族中的码是 F最优的。请注意，文献 [16] 中构造的长度为 $n=9$ 且基数最大的码有 171 个自由点，而我们的码有 177 个自由点。

$n=6$	基数 M	12	11	10	9	8
	自由点 F	16	23	28	33	38
$n=7$	基数 M	18	17	16	15	14
	自由点 F	48	56	62	68	73
$n=8$	基数 M	36	35	34	33	32
	自由点 F	76	85	92	99	106
$n=9$	基数 M	62	61	60	59	58
	自由点 F	177	186	193	200	207

表 II （n， M， 1） 码的最优自由点数。

长度与基数	重量分布
$n=6, M=12$	1+0+3+4+3+0+1
$n=7, M=18$	1+0+3+5+5+3+1+0
$n=7, M=17$	1+0+3+5+6+1+1+0
$n=8, M=36$	1+0+4+8+10+8+4+0+1
$n=9, M=62$	1+0+4+9+17+17+11+2+1+0

表 III 最优重量分布。

有了带自由点的码表，我们便可应用定理 1，为带反馈的非对称信道构造传输策略。当参数 $M(v)$ 和 $F(v)$ 仅取决于码字重量时，可得如下结果。

推论 2. 设对于所有满足 $v\in V$ 中符号 1 的数量为 w 的 $v\in V$，均有 $M(v)=M_w$ 和 $F(v)=F_w$，即 $M(v)$ 和 $F(v)$ 仅取决于码字 v 的重量。若条件

$$(n_1-w)M_{w+1}\le F_w \tag{4}$$

*ar*对所有 $w\in[0,n_1-1]$ 均成立，则传输消息的数量为

$$M=\sum_{w=0}^{n_1}\binom{n_1}{w}M_w. \tag{5}$$

基于推论 2 和定理 1 构造的算法所传输的消息数量见表 IV。为了计算出能得出最优答案的 M_w 和 F_w 的取值，我们采用了

动态规划技术。在下文给出的示例中，我们详细介绍了分别使用推论 2 和定理 1 针对长度为 $n=9$ 和 $n=8$ 得到的码。

n	5	6	7	8	9	10	11	12	13
M (推论 2)	9	16	29	52	96	177	327	607	1120
M (定理 1)	9	16	29	53	97	≥ 177	≥ 329	≥ 607	≥ 1120

表 IV 使用一次反馈和单个错误的非对称信道中传输的消息数量。

我们将用 $(n, M, F, t)_Z$ 表示一种长度为 n、可纠正 t 个非对称错误且具有 M 个码字和 F 个自由点的非自适应码。在第一个示例中，我们展示推论 2 的一种应用：反馈后使用的码仅取决于反馈前发送的码字的重量。在长度为 $n=8$时，应用推论 2 只能传输 52 条消息。在第二个示例中，我们展示如何使用定理 1 传输 53 条消息。这意味着推论 2 并非总能给出最优答案。

示例 1。 $n=9$ 和 $M=96$。

设 $n_1=5$ 和 $n_2=4$。对于对应于重量为 0 和 1 的二进制字的顶点，我们分配一个含有两个码字 $\{0000, 0011\}$ 的 $(4, 2, 12, 1)_Z$ 码。对于重量为 2 和 3 的顶点，我们分配一个含有三个码字 $\{0000, 0011, 1100\}$的 $(4, 3, 9, 1)_Z$ 码。对于重量为 4 和 5 的顶点，我们分配一个含有四个码字 $\{0000, 0011, 1100, 1111\}$的 $(4, 4, 4, 1)_Z$码。

让我们检查 $w \in [0, 4]$ 的约束 $(n_1 - w)M_{w+1} \leq F_w$：

$$\begin{aligned} w=0:&\ 5\cdot 2 \leq 12,\\ w=1:&\ 4\cdot 3 \leq 12,\\ w=2:&\ 3\cdot 3 \leq 9,\\ w=3:&\ 2\cdot 4 \leq 9,\\ w=4:&\ 1\cdot 4 \leq 4. \end{aligned}$$

利用 (5)，我们计算传输消息的数量：

$$1\cdot 2 + 5\cdot 2 + 10\cdot 3 + 10\cdot 3 + 5\cdot 4 + 1\cdot 4 = 96.$$

例 2。 $n=8$ 和 $M=53$。

令 $n_1=6$ 和 $n_2=2$。我们为顶点 111111 分配一个 $(2, 2, 0, 1)_Z$ 码 $\{00, 11\}$。我们为顶点 111000、001110、010101、100011、100100、010010、001001、110000、010100、001000、000010 和 000001 分配一个含有 0 个码字的 $(2, 0, 4, 1)_Z$码。我们为所有其他顶点分配一个含有一个码字的 $(2, 1, 3, 1)_Z$码 $\{00\}$。很容易验证，定理 1 的条件 (2) 得到了满足。例如，让我们检查顶点 $v=101000$ 的条件：总共有四个顶点可以到达 v： $\{111000, 101100, 101010, 101001\}$。相应码的基数为

$$\begin{aligned} M(111000)&=0, \qquad M(101100)=1,\\ M(101010)&=1, \qquad M(101001)=1. \end{aligned}$$

这些基数的总和不大于 $F(101000) = 3$；也就是说，顶点$v=101000$ 的约束得到满足。同样，可以检查其他顶点的约束。

传输消息总数为 $2+0+51=53$。

我们给出一张表，列出了在存在单个非对称错误且具有完全反馈的信道中可传输的消息数量。最优结果见 [11], , 其中传输 $M=2^m$ 条消息所需的长度为 $n=m-1+\lceil \log_2(m+3) \rceil$。尽管我们只使用一次反馈，但除了 $n=7$的情况外，对于 $n \leq 13$，我们能传输的消息数量多于 [11] 中的结果。对于一种

具有完全反馈且存在单个错误的非对称信道，可以采用一种类似于 DADA 的算法，构造出传输消息数量达到最优值 M_{ad} 的码。这些码的基数列于表V。后续论文之一将详细介绍这类码的构造方法。

n	5	6	7	8	9	10	11	12	13
M [11]	8	16	32	32	64	128	256	512	1024
M_{ad}	11	20	36	66	121	223	415	774	1452

表V 完全反馈且存在单个错误的非对称信道的码基数。

经费支持

I.V. Vorobyev 的研究部分得到了俄罗斯基础研究基金会和保加利亚国家科学基金会联合资助（项目编号：20-51-18002）、俄罗斯基础研究基金会资助（项目编号：20-01-00559）以及 BMBF-NEWCOM 资助（编号：16KIS1005）的支持。

K. Deppe 的研究部分得到了 BMBF-NEWCOM（资助编号：16KIS1005）和 BMBF-6G-life（资助编号：16KISK002）的支持。

A.V. Lebedev 和 V.S. Lebedev 的研究部分得到了俄罗斯基础研究基金会与保加利亚国家科学基金会联合资助（项目编号：20-51-18002）的支持。

参考文献

[1] R´enyi，A.，《信息论中的一个问题》，Magyar Tud. Akad. Mat. Kutat´o Int. K¨ozl.，1961年，第6卷，第505–516页。[2] Berlekamp，E.R.，《无噪声、无延迟反馈下二元对称信道的分组编码》，载于《纠错码》（美国陆军数学研究中心于1968年5月6–8日在威斯康星大学麦迪逊分校主持召开的会议论文集），Mann，H.B. 编，纽约：威利，1969年，第61–85页。[3] Zigangirov，K.Sh.，《带反馈的二元对称信道传输中可纠正错误的数量》，Probl. Peredachi Inf.，1976年，第12卷，第2期，第3–19 [Probl. Inf. Transm.（英文译本），1976年，第12卷，第2期，第85–97]页。[4] Ulam，S.M.，《一位数学家的冒险》，纽约：斯克里布纳，1976年。[5] Pelc，A.，《带谎言搜索中的乌拉姆问题的解》，J. Combin. Theory Ser. A，1987年，第44卷，第1期，第129–140页。[6] Guzicki，W.，《带两个谎言的乌拉姆搜索游戏》，J. Combin. Theory Ser. A，1990年，第54卷，第1期，第1–19页。[7] Deppe，C.，《带三个谎言的乌拉姆搜索游戏的解，或二元三错纠正码的最优自适应策略》，Discrete Math.，2000年，第224卷，第1–3期，第79–98页。[8] desJardins，D.L.，《无噪声反馈下的精确编码》，博士论文，数学系，加州大学伯克利分校，2002年。可查阅[9] Rivest，R.L.、Meyer，A.R.、Kleitman，D.J.、Winkelmann，K. 和 Spencer，J.，《应对二分搜索过程中的错误》，J. Comput. System Sci.，1980年，第20卷，第3期，第396–404页。[10] Cicalese，F.，《容错搜索算法：不可靠信息下的可靠计算》，柏林：施普林格，2013年。[11] Cicalese，F. 和 Mundici，D.，《一个非对称错误下的最优编码：低于球形堆积界》，载于《计算与组合数学》（第六届 COCOON 2000 年度国际会议论文集，澳大利亚悉尼，2000年7月26–28日），Du，D.Z.、Eades，P.、Estivill-Castro，V.、Lin，X. 和 Sharma，A. 编，Lect. Notes Comput. Sci.，第1858卷，柏林：施普林格，2000年，第159–169页。[12] Dumitriu，I. 和 Spencer，J.，《半说谎者游戏》，Theoret., Comput Sci.，2004年，第313卷，第3期，第353–369页。[13] Spencer，J. 和 Yan，C.H.，《半说谎问题》，J. Combin. Theory Ser. A，2003年，第103卷，第1期，第69–89页。[14] Bassalygo，L.A.，《带一次无错反馈的非二元纠错码》，Probl. Peredachi Inf.，2005年，第41卷，第2期，第63–67 [Probl. Inf. Transm.（英文译本），2005年，第41卷，第2期，第125–129]页。[15] Dumitriu，I. 和 Spencer，J.，《任意信道上的两批次说谎游戏》，SIAM J. Discrete Math.，2005年，第19卷，第4期，第1056–1064页。[16] Delsarte，P. 和 Piret，P.，《二元非对称纠错码的界与构造》，IEEE Trans. Inform. Theory，1981年，第27卷，第1期，第125–128页。[17] Kløve，T.，《纠正非对称错误的码的上界》，IEEE Trans. Inform. Theory，1981年，第27卷，第1期，第128–131页。[18] Weber，J.、de Vroedt，C. 和 Boekee，D.，《纠正非对称错误的码的新上界》，IEEE Trans. Inform. Theory，1987年，第33卷，第3期，第434–437页。