信息销售的最优机制设计

数据要素处理基础

Author: Forliage

Email: masterforliage@gmail.com

Date: June 30, 2025

College: 计算机科学与技术学院

浙江大学
ZHEJIANG UNIVERSITY

Abstract

Contents

1 引言 (Introduction)

1.1 信息市场的兴起

在当今的数字时代，信息本身已成为一种至关重要的商品。其交易规模和速度在人类商业史上达到了前所未有的水平。大型科技公司、数据经纪商（如 Bluekai, Acxiom, Experian）以及专业的咨询机构，其核心业务就是收集、处理并销售各类信息。这些信息的应用场景无处不在：

- **在线广告**:广告平台向广告商出售用户的人口统计学数据、兴趣标签、历史行为等信息，以帮助广告商实现精准投放，将运动汽车的广告展示给富裕的年轻单身用户，而将家庭MPV的广告推送给有孩子的中年用户。
- **金融信贷**:银行和金融机构购买个人的信用报告和消费数据，以评估其信用风险，从而决定是否批准贷款以及贷款的利率。
- **商业咨询**:咨询公司利用其行业洞察和市场分析（即信息），为企业客户的重大决策（如是否进入新市场、是否收购竞争对手）提供建议并收取高额费用。

这些场景的共同点是：存在一个信息的买方（广告商、银行、企业客户）和一个信息的卖方（数据平台、征信机构、咨询公司）。买方需要利用卖方的信息来做出一个更优的决策，从而获得更高的收益。而作为垄断性的卖方，其目标则是设计一个巧妙的“游戏规则”（即机制），来最大化自己从信息销售中获得的收益。

本报告的核心目标，就是深入探讨这个“游戏规则”应该如何设计。我们将建立一个严谨的数学模型，来分析和解答以下问题：

1. 如何量化信息的价值？
2. 最优的信息销售策略（机制）是怎样的？
3. 销售信息与销售实体商品（比如一个面包、一台电脑）的根本区别在哪里？
4. 这些区别又将如何影响机制的设计？

1.2 一个具体例子：广告商的困境

为了让讨论更加具体，让我们始终将一个生动的例子放在心中：

场景:一家汽车制造商（买方）希望在一个广告位上投放一则广告。它有两种广告素材可选：

- **广告A**:宣传一款新潮的跑车。
- **广告B**:宣传一款宽敞的家庭MPV。

广告的效果取决于浏览该广告位的用户特征，而这些特征对汽车制造商来说是未知的。我们称用户的真实类型为一个未知的 **世界状态**ω。例如，ω可以是"年轻单身"或"中年有孩"。

一家数据提供商（卖方），例如网站的运营方，掌握了关于该用户的一些精确信息，比如通过用户注册信息知道其年龄和婚姻状况。因此，卖方知道ω。

与此同时，汽车制造商（买方）自己也并非一无所知。它可能通过追踪用户在其官网上的浏览记录，得到一些关于用户偏好的线索。例如，用户之前浏览过跑车页面。我们将买方自己掌握的这部分私有信息称为其**私有类型**θ。

现在，数据提供商（卖方）希望将自己掌握的用户精确信息ω。卖给汽车制造商（买方），并尽可能多地收费。而汽车制造商则希望根据卖方提供的信息以及自己的信息θ，选择最合适的广告（A或B），以最大化广告带来的销售转化收益。

在这个例子中，所有关键元素都已齐备：卖方、买方、双方的私有信息(ω和θ)、买方的决策（投放广告A或B），以及决策的收益。我们的任务就是站在卖方的角度，设计一个最优的销售方案。

1.3 核心挑战：信息销售为何与众不同

如果我们试图将销售实体商品的逻辑直接套用到信息销售上，会立刻遇到障碍。销售信息和销售一个面包有着本质的不同，这些不同点构成了本领域研究的核心挑战。

1. **“产品”形态的无限复杂性 (Complex "Bundles")**

- **实体商品：**一个面包店主可以决定是单独卖面包，还是将面包和牛奶捆绑销售。产品的组合方式是有限的。
- **信息商品：**一个掌握了n比特信息的卖方，能“制造”出无穷无尽的“信息产品”。她可以出售完整n比特信息，也可以出售其中的某个子集，甚至可以出售这n比特信息的某种函数变换，例如“前两个比特的异或（XOR）值是1”。这种灵活性使得最优机制的设计空间变得异常庞大。

2.**消费前价值未知 (Value is Unknown Before Consumption)**

- **实体商品:**一个饥饿的人在买面包之前，就已经很清楚这个面包能给他带来的价值（填饱肚子）。
- **信息商品：**信息的价值恰恰在于其内容本身。在买方真正“看到”信息内容之前，他无法准确评估这则信息对他决策的帮助有多大。这引发了一个严重的承诺问题：如果卖方先把信息透露给买方，买方一旦获知了信息，就没有动力再为此付费了。这在经济学上被称为“霍尔德普问题”（Hold-up Problem）。

3.**价格本身传递信息 (Price Reveals Information)**

- **实体商品：**根据经典的机制设计理论（如税收原理），许多复杂的拍卖机制可以被简化为给每种商品或商品组合定一个价格。买方面对的是一个价格菜单，其报价与买方的类型无关。

- **信息商品：** 在信息销售中，如果卖方制定的价格依赖于她所掌握的信息ω，那么价格本身就成了一个信号，会向买方泄露关于ω的信息。想象一下，在我们的汽车广告例子中，如果卖方说："这则信息我卖1000元"，买方可能会推断"通常只有用户信息价值很高（比如是高净值客户）时，卖方才会定这么高的价"，从而在付费前就免费获得了一部分有价值的信息。

这些挑战决定了信息销售机制的设计必须更加精巧和复杂，简单的"一口价"策略通常远非最优。我们需要一个更通用的框架来描述买卖双方之间可能的互动过程。

1.4 研究目标：设计最优机制

本报告的核心是研究一个垄断卖方（只有一个卖家）如何向一个单一买方销售信息以实现收益最大化。我们将这个问题置于一个通用的博弈论框架下，其中：

- 卖方设计一个交互协议（或称为机制）。
- 卖方承诺会遵守这个协议。
- 买方则是理性的，他会根据自己的利益决定如何参与协议（可能谎报自己的信息，也可能中途退出）。
- 我们还会引入一个更现实的约束：预算限制。即买方和卖方的支付能力都是有限的。

我们的目标是找到那个能为卖方带来最大期望收益的最优机制，并研究这个机制的结构、性质以及计算它的算法。

2 问题的形式化 (Formalizing the Problem)

为了能够严谨地分析信息销售问题，我们首先需要建立一个统一的数学语言。

2.1 核心要素：上下文 (Context)(u, μ)

整个信息销售问题可以被一个我们称为上下文（Context）的元组(u, μ)所概括。这个上下文是买卖双方的共同知识（Common Knowledge）

它包含以下核心要素：

世界状态 (State of the World)： $\omega \in \Omega$。这是一个随机变量，代表了客观世界中一个不确定的、但与决策收益相关的状态。 Ω是所有可能状态的有限集合。

卖方私有信号 (Seller's Private Signal)： 在本模型的基本设定中，我们假设卖方完全知晓世界状态ω。所以，ω就是卖方的私有信息。

买方私有类型 (Buyer's Private Type)： $\theta \in \Theta$。这也是一个随机变量，代表了买方在交易开始前就拥有的私有信息。Θ是所有可能类型的有限集合。θ可以包含多种信息：

1. 买方关于ω的信号：θ可能是ω的一个不完美的、带有噪声的观测。
2. 买方的偏好：θ也可以代表买方自身的效用函数差异。我们统一用θ来表示买方所有的私有信息。

买方行动 (Buyer's Actions)：$a \in A$。这是买方在获得信息后可以选择的决策集合，A是一个有限集。

效用函数 (Utility Function)：$u(\theta, \omega, a) \to \mathbb{R}$。这个函数描述了买方的收益。当买方的私有类型是$\theta$，世界真实状态是$\omega$，且买方采取了行动$a$时，他获得的收益是$u(\theta, \omega, a)$。这个函数是整个模型的核心，它将信息和行动的价值联系了起来。

联合概率分布 (Joint Probability Distribution)：$\mu(\omega, \theta)$。这是一个在$\Omega \times \Theta$上的联合概率分布，是所有参与者的共同知识。$\mu(\omega, \theta) = \Pr(\text{世界状态} = \omega, \text{买方状态} = \theta)$。这个分布描述了卖方和买方私有信息之间的相关性。如果$\mu(\omega, \theta) = \mu(\omega)\mu(\theta)$，我们称卖方和买方信号独立。否则，称之为相关。例如，如果富有的买方（一种θ）更有可能是跑车爱好者（一种ω），那么ω和θ就是相关的。

2.2 买方的目标：最大化效用

一个理性的买方，其目标是在其所知信息的约束下，选择一个行动a来最大化自己的期望效用。

无额外信息时的期望效用 (Status Quo Utility)

在与卖方交易之前，类型为θ的买方只知道自己的θ。他需要基于θ对ω形成一个后验信念。根据贝叶斯法则，ω的条件概率分布是$\Pr(\omega|\theta) = \mu(\omega, \theta)/\mu(\theta)$，其中$\mu(\theta) = \sum_{\omega'} \mu(\omega', \theta)$。因此，他的最优决策是选择一个$a$来最大化期望效用：

$$U_{prior}(\theta) = \max_{a \in A} \mathbb{E}_{\omega \sim \mu(*|\theta)}[u(\theta, \omega, a)] = \max_{a \in A} \sum_{\omega \in \Omega} \frac{\mu(\omega, \theta)}{\mu(\theta)} u(\theta, \omega, a)$$

这是买方的保留效用（Reservation Utility）或外部选项（Outside Option），即他不参与交易所能获得的最低保证效用。

拥有完全信息时的期望效用 (Full Information Utility)

假设一个理想情况，卖方免费将信息ω完整地告诉了买方。那么对于每一个可能的ω，买方都可以选择最优的行动a。他此时的期望效用是：

$$U_{post}(\theta) = \mathbb{E}_{\omega \sim \mu(*|\theta)}[\max_{a \in A} u(\theta, \omega, a)] = \sum_{\omega \in \Omega} \frac{\mu(\omega, \theta)}{\mu(\theta)} \max_{a \in A} u(\theta, \omega, a)$$

信息的价值 (Value of Information)

对一个类型为θ的买方而言，信息ω的全部价值$\xi(\theta)$，就是拥有信息前后他能获得的最大

期望效用之差：

$$\xi(\theta) = U_{post}(\theta) - U_{prior}(\theta) \geq 0$$

这个差值$\xi(\theta)$是非负的，因为拥有更多信息总不会让决策变得更差。$\xi(\theta)$代表了类型为 θ的买方愿意为获得完整信息ω所支付的最高价格。如果价格超过$\xi(\theta)$，他宁愿不要这个信息，自己根据θ去猜。

2.3 卖方的目标：最大化收益

卖方的目标是设计一个销售机制，从买方那里榨取尽可能多的价值。其总的期望收益（Revenue）是所有类型的买方支付的金额的期望值：

$$\text{Revenue} = \sum_{\theta \in \Theta} \mu(\theta) \cdot t(\theta)$$

其中$t(\theta)$是卖方最终从类型为θ的买方那里收取的期望费用。显然，卖方收取的费用不能超过信息的价值，即 $t(\theta) \leq \xi(\theta)$。卖方的挑战在于，她并不知道买方的真实类型$\theta$，所以她无法为每种类型“量身定做”一个价格 $\xi(\theta)$。她必须设计一个对所有类型都有效的机制。

2.4 初步尝试：“密封信封”机制 (The "Sealed Envelope" Mechanism)

在深入复杂的机制之前，我们先分析一个最直观、最简单的方案，并看看它有什么问题。

机制描述：

1. 卖方知道了真实的ω。
2. 她将ω的值写在一张纸条上，放入一个信封。
3. 她给这个信封定一个固定的、公开的价格t。
4. 买方看到价格t后，自行决定是否购买。

买方的决策：一个类型为θ的买方，其购买此信封的价值是$\xi(\theta)$。根据理性人假设，他会做出如下决策：

1. 如果$\xi(\theta) \geq t$，他会购买。购买后，他的净效用是$\xi(\theta) - t$。
2. 如果$\xi(\theta) < t$，他不会购买。他不购买的净效用是 0。为简化讨论，我们假设在$\xi(\theta) = t$时买方会购买。）

卖方的收益：卖方的期望收益是价格t乘以所有会购买的买方类型的概率之和：

$$\text{Revenue}(t) = t \cdot \sum_{\theta \text{ s.t. } \xi(\theta) \geq t} \mu(\theta)$$

卖方的任务就变成了选择一个最优的价格t^*来最大化这个收益函数Revenue(t)。这本质上是一个经典的垄断定价问题。

“密封信封”机制的缺陷：这个机制看起来简单，但它忽略了一个关键问题：卖方在得知ω之后，可能会希望根据ω的不同来调整价格t。

一个失败的改进尝试：卖方可能会想：“对于不同的ω，信息ω对买方的价值可能是不同的。我为什么不根据ω来定价呢？”，即设置一个价格函数$t(\omega)$。

这恰恰是信息销售的微妙之处。一旦卖方这么做了，价格本身就携带了关于ω的信息。

假设在广告例子中，$\omega =$年轻单身时信息价值高，卖方定价t(年轻单身)$= 1000$元；$\omega =$ 中年有孩时信息价值低，卖方定价t(中年有孩) $= 100$元。买方过来一询价，卖方报价“1000元”。此时，即使买方一分钱没付，他也立刻能推断出 ω极有可能是“年轻单身”。他已经免费获得了信息，为什么还要付费呢？

这个简单的例子揭示了设计信息销售机制的核心困难：任何与卖方私有信息ω相关的机制元素（如价格、信息披露的颗粒度等），都可能成为泄露信息的渠道。买方可以利用这些渠道进行“投机”，在不完全付费的情况下获取信息。

因此，我们需要一个更强大、更通用的框架来描述和分析所有可能的、包含复杂交互的销售协议。

2.5 示例

为了更具体地理解$\xi(\theta)$的计算和“密封信封”机制的收益，我们可以用Python写一个简单的模拟。

场景设定：

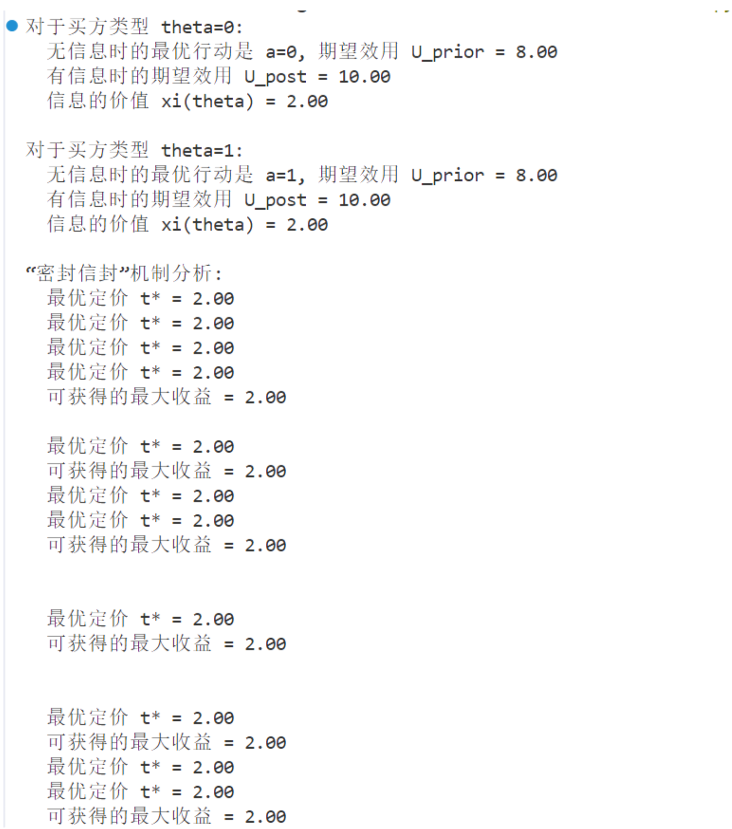
- 世界状态$\Omega = 0, 1$
- 买方状态$A = 0, 1$
- 买方类型$\Theta = 0, 1$
- 联合分布$\mu(\omega, \theta)$:
  - $\mu(\omega = 0, \theta = 0) = 0.4$
  - $\mu(\omega = 1, \theta = 0) = 0.1$
  - $\mu(\omega = 0, \theta = 1) = 0.1$
  - $\mu(\omega = 1, \theta = 1) = 0.4$
  - 这表明θ是ω的一个强信号，$\theta = 0$暗示$\omega = 0$，$\theta = 1$暗示$\omega = 1$。
- 效用函数$u(\theta, \omega, a)$：假设效用只和ω与a是否匹配有关，θ只影响买方的先验信念。
  - $u(\omega, a) = 10$ 如果$\omega = a$(行动正确)
  - $u(\omega, a) = 0$如果$\omega \neq a$(行动错误)

以下是实现的Python代码，完整的程序在同级目录下的program1.py程序。

```python
import numpy as np
import matplotlib.pyplot as plt

class Context:
    def __init__(self):
        self.Omega = [0, 1]
        self.Theta = [0, 1]
        self.A = [0, 1]

        self.mu_joint = np.array([[0.4, 0.1],  # theta=0: mu(w=0|t=0)=0.4, mu(w=1|t=0)=0.1
                                  [0.1, 0.4]]) # theta=1: mu(w=0|t=1)=0.1, mu(w=1|t=1)=0.4

        self.mu_theta = np.sum(self.mu_joint, axis=0) # [0.5, 0.5]
        self.mu_omega = np.sum(self.mu_joint, axis=1) # [0.5, 0.5]

        self.mu_cond_w_given_t = self.mu_joint / self.mu_theta

    def u(self, omega, action):
        return 10.0 if omega == action else 0.0

def calculate_xi(context, theta):

    expected_utilities_prior = []
    for action in context.A:
        utility = 0
        for omega_idx, omega in enumerate(context.Omega):
            prob_w = context.mu_cond_w_given_t[omega_idx, theta]
            utility += prob_w * context.u(omega, action)
        expected_utilities_prior.append(utility)

    u_prior = np.max(expected_utilities_prior)
    best_action_prior = np.argmax(expected_utilities_prior)

    u_post = 0
    for omega_idx, omega in enumerate(context.Omega):
```

```
            prob_w = context.mu_cond_w_given_t[omega_idx, theta]

            best_utility_for_omega = 0
            for action in context.A:
                best_utility_for_omega = max(best_utility_for_omega
                    , context.u(omega, action))

            u_post += prob_w * best_utility_for_omega

    xi = u_post - u_prior
    return xi

def sealed_envelope_revenue(t, xi_values, mu_theta):
    revenue = 0
    for theta_idx, xi in enumerate(xi_values):
        if xi >= t:
            revenue += t * mu_theta[theta_idx]
    return revenue

if __name__ == "__main__":
    ctx = Context()

    xi_values = [calculate_xi(ctx, theta) for theta in ctx.
       Theta]

    prices_to_test = np.linspace(0, max(xi_values) + 1, 1000)
    revenues = [sealed_envelope_revenue(t, xi_values, ctx.
       mu_theta) for t in prices_to_test]

    max_revenue = np.max(revenues)
    optimal_price = prices_to_test[np.argmax(revenues)]

    plt.figure(figsize=(10, 6))
    plt.plot(prices_to_test, revenues)
    plt.title("Revenue of Sealed Envelope Mechanism vs. Price (
       t)")
    plt.xlabel("Price (t)")
    plt.ylabel("Expected Revenue")
    plt.axvline(x=optimal_price, color='r', linestyle='--',
       label=f'Optimal Price t* = {optimal_price:.2f}')
    plt.grid(True)
```

```
        plt.legend()
        plt.show()
```



```
对于买方类型 theta=0:
  无信息时的最优行动是 a=0, 期望效用 U_prior = 8.00
  有信息时的期望效用 U_post = 10.00
  信息的价值 xi(theta) = 2.00

对于买方类型 theta=1:
  无信息时的最优行动是 a=1, 期望效用 U_prior = 8.00
  有信息时的期望效用 U_post = 10.00
  信息的价值 xi(theta) = 2.00

"密封信封"机制分析:
  最优定价 t* = 2.00
  最优定价 t* = 2.00
  最优定价 t* = 2.00
  最优定价 t* = 2.00
  可获得的最大收益 = 2.00

  最优定价 t* = 2.00
  可获得的最大收益 = 2.00
  最优定价 t* = 2.00
  最优定价 t* = 2.00
  可获得的最大收益 = 2.00


  最优定价 t* = 2.00
  可获得的最大收益 = 2.00


  最优定价 t* = 2.00
  可获得的最大收益 = 2.00
  最优定价 t* = 2.00
  最优定价 t* = 2.00
  可获得的最大收益 = 2.00
```

Figure 1. Result

代码运行结果如下：

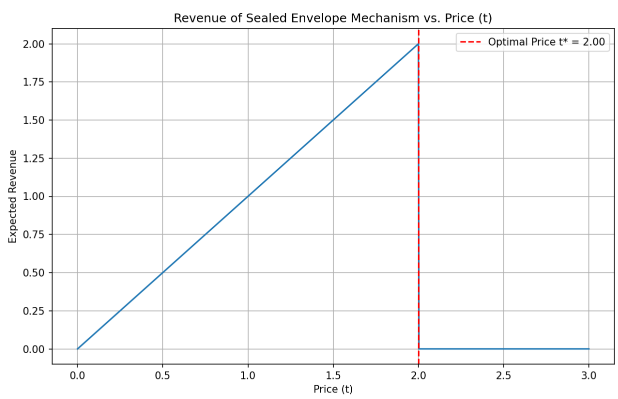


Figure 2. Visualization

在这个特定的例子中，两种类型的买方$\theta = 0$和$\theta = 1$恰好具有相同的信息价值$\xi(\theta) = 2.0$。因此，卖方最优的定价就是$t^* = 2.0$，此时两种类型的买方都会购买，卖方的总收益为

$$t^* \times (\mu(\theta = 0) + \mu(\theta = 1)) = 2.0 \times (0.5 + 0.5) = 2.0$$

这个简单的代码示例，将前面定义的抽象概念（上下文、效用、信息价值）转化为了可计算的实体，并直观地展示了最简单的“密封信封”机制是如何运作和优化的。然而，正如我们所分析的，这个简单机制的背后隐藏着深刻的缺陷，这促使我们必须进入下一章，探索更一般、更强大的机制。

3 通用交互协议与显示原理 (General Protocols and the Revelation Principle)

3.1 描述一切可能：通用交互协议 (Generic Interactive Protocol)

为了不遗漏任何可能的销售策略，我们需要一个能囊括所有互动方式的通用模型。这个模型就是通用交互协议，它可以被想象成一个多回合的、动态的博弈树。

定义3.1(通用交互协议)：一个通用交互协议是一个有限的决策树，由一系列节点 (Node) 和连接节点的边 (Edge) 构成。树中的非叶子节点分为三类：

1. 卖方节点 (Seller Node)：轮到卖方行动。
   - 在卖方节点n，卖方会根据她的私有信息ω，以一定的概率选择一条边（即发送一个信号）通往下一个节点。
   - 形式化地，对于节点n的每一个子节点c，卖方都预先设定了一个概率$p_n(\omega, c)$，表示当她自己的信号是ω时，她选择走向子节点c的概率。
   - 对于任意ω，必须有$\sum_c p_n(\omega, c) = 1$。
2. 买方节点 (Buyer Node)：轮到买方行动。
   - 在买方节点n，买方会根据他的私有类型θ（以及在预算约束模型中的预算b）来决定走向哪个子节点。
   - 买方的策略ϕ是一个函数，它将买方的类型(θ, b)和当前节点n映射到一个关于子节点的概率分布。
3. 支付节点 (Transfer Node)：发生资金转移。
   - 支付节点n只有一个子节点。
   - 与每个支付节点n相关联的是一个固定的金额$t(n)$。
   - 当协议路径经过此节点时，一笔金额为$t(n)$的支付从买方转移给卖方。
   - 如果$t(n)$是负数，则表示卖方向买方支付了$|t(n)|$。

协议的执行过程：协议从根节点开始。根据当前节点的类型（卖方、买方或支付），某一方行动或发生支付，协议状态转移到下一个节点。这个过程持续进行，直到到达一个叶子节点 (Leaf Node)。

在到达叶子节点1时，整个交互结束。买方根据从根节点到叶子节点1的整条路径上观察到的所有卖方行动（即收到的所有信号），形成对ω的最终后验信念。然后，他基于这个后验

信念选择一个最优的行动a来最大化自己的期望效用。

3.2 机制设计的基石：显示原理 (The Revelation Principle)

显示原理是机制设计领域最核心的定理之一。它的思想是，任何复杂的、间接的机制，其最终达成的效果，都可以通过一个简单得多的直接显示机制 (Direct Revelation Mechanism) 来实现，并且收益不会降低。

定义 3.2 (直接显示机制):一个直接显示机制是一种特殊的协议，其结构非常简单：

1. 协议的根节点是一个买方节点。
2. 在这个节点，买方被要求直接报告他的私有类型θ（以及预算b）。
3. 树中没有其他的买方节点。买方只行动一次，就是在一开始“自报家门”。
4. 机制（现在由卖方扮演）根据买方报告的类型$(\hat{\theta}, \hat{b})$，以及自己掌握的ω，来执行后续的支付和信息披露。

定理 3.1 (显示原理，信息销售版):假设存在一个任意复杂的通用交互协议Π，以及在该协议下一个理性的买方最优策略ϕ，这个组合(Π, ϕ)能为卖方带来期望收益R。那么，必然存在一个直接显示机制Π_d，在该机制下，买方如实报告自己的真实类型(θ, b)是其最优策略（我们称之为激励相容 Incentive Compatible, IC），并且这个直接机制能为卖方带来至少为R的期望收益。

显示原理的直觉证明 (Proof by Simulation)。这个定理的证明非常有启发性，其核心思想是模拟。

假设我们有一个复杂的、多回合的旧机制Π。我们可以构造一个新的直接机制Π_d如下：

1. 新机制Π_d的第一步，是请买方报告他的类型θ。
2. 一旦买方报告了$\hat{\theta}$，新机制（卖方）就在自己的“后台”开始模拟旧机制Π的整个过程。当在旧机制中轮到买方行动时，新机制就查阅买方在旧机制下的最优策略$\phi(\hat{\theta})$，然后代替买方做出那个选择。当轮到卖方行动时，新机制就按照旧机制的规则行动。
3. 新机制在后台完整地模拟完一遍旧机制，得到一个最终的 outcome（包括给买方的信息和买方需要支付的总金额）。然后，新机制直接把这个最终 outcome 交给买方。

为什么买方愿意如实报告？

因为如果他撒谎，比如他的真实类型是θ，却报告了$\hat{\theta}$。那么新机制就会按照$\hat{\theta}$的最优策略$\phi(\hat{\theta})$去模拟。这等价于，在旧机制Π中，一个类型为θ的买方，假装自己是$\hat{\theta}$来玩游戏。但我们已经假设了$\phi(\theta)$是类型为θ的买方在旧机制中的最优策略，所以假装成别人$(\hat{\theta})$来玩，对他来说收益不会更高。因此，在新机制中，他没有动力撒谎，如实报告是他的最优选择。

显示原理极大地简化了我们的问题。我们不再需要在所有可能的、奇形怪状的协议树中进行搜索，而只需要在一类结构非常简单的直接机制中寻找最优者。在直接机制中，我们只需要决定两件事：

1. 分配规则：对于每一种可能的报告$(\hat{\theta}, \hat{b})$和真实的ω，卖方应该向买方披露什么样的信息？
2. 支付规则：对于每一种可能的报告$(\hat{\theta}, \hat{b})$和真实的ω，卖方应该向买方收取多少钱？

3.3 更进一步：单轮显示机制 (One-Round Revelation)

在许多经典的机制设计问题（如商品拍卖）中，显示原理还能被加强。不仅买方只需要报告一次，整个支付和分配过程也可以在"一轮"内完成。然而，在信息销售中，情况变得微妙起来。

定义 3.3 (单轮显示机制):一个单轮显示机制是一个深度最多为3的直接显示机制。其路径通常是：

$$\text{买方报告类型} \rightarrow \text{支付发生} \rightarrow \text{卖方披露信息}$$

或者

$$\text{买方报告类型} \rightarrow \text{卖方披露信息} \rightarrow \text{支付发生}$$

核心问题：对于信息销售问题，最优机制是否总能简化为单-轮的显示机制？答案是：不一定。这取决于买方的承诺和信号的相关性。

定理 3.2 (单轮机制的充分条件)：在以下两种情况中，任何机制（无论多复杂）的收益，都可以被一个单轮显示机制所实现：

1. 当买方是承诺的 (Committed Buyer)。
2. 当买方不承诺，但卖方信号ω和买方类型θ是相互独立的。

证明思路 (Case 1: Committed Buyer)当买方是承诺的时候，他不能中途退出。我们可以构造一个单轮机制如下：

1. 买方报告类型θ。
2. 机制（卖方）根据θ和自己的ω，在后台模拟完整个原始协议。
3. 在模拟过程中，机制会记录下所有需要发生的支付，并计算出总支付额 t_total。同时，它也会计算出最终应该披露给买方的信息 s_final。
4. 模拟结束后，机制直接向买方收取 t_total，并同时把 s_final 给他。由于买方是承诺的，他必须接受这个最终结果。这个过程等价于原始协议，并且显然是单轮的。

证明思路 (Case 2: Uncommitted but Independent Signals) 当信号独立时$\mu(\omega, \theta) = \mu(\omega)\mu(\theta)$,买方对$\omega$的先验信念$\mu(\omega)$与其自身类型$\theta$无关。这意味着，无论买方报告自己是$\theta$还是$\hat{\theta}$,机制在计算期望支付时，都是对同一个$\omega$的分布$\mu(\omega)$求期望。我们可以构造一个单轮机制：

1. 买方报告类型θ。
2. 机制计算出，如果买方类型真的是θ，那么在原始协议中他的期望支付额是多少，记为$\mathbb{E}[t|\theta]$。

3. 机制先向买方收取$\mathbb{E}[t|\theta]$。
4. 然后，机制再根据ω和买方报告的θ，模拟原始协议中的信息披露部分，并将最终信息给买方。

这个机制是可行的，因为支付发生在信息披露之前，不承诺的买方没有机会“白看”信息。而由于信号独立，一个类型为θ的买方谎报成$\hat{\theta}$,并不会改变他对支付额的期望（因为都是对$\mu(\omega)$求期望），所以他欺骗的动机只剩下获取信息上的好处，而这在原始协议中已经被保证为不划算的。

当单轮显示原理失效时.关键洞察：当买方不承诺且信号相关时，单轮显示原理失效！原因：在这种情况下，上面两种构造方法都行不通了。

- 先披露信息，后收费：行不通。不承诺的买方拿到信息后会直接跑路。
- 先收费，后披露信息：也行不通。收费多少呢？我们不能像独立信号时那样收取期望支付。因为信号是相关的，一个真实类型为θ的买方，如果他谎报成$\hat{\theta}$,他对ω的信念是$\mu(\omega|\theta)$，而机制是按$\mu(\omega|\hat{\theta})$来计算期望支付的。这两个期望值不同，导致买方可以通过谎报来操纵他需要预付的费用。

结论：在这种最复杂的情况下，为了实现最优收益，卖方可能必须采取一种“挤牙膏”式的策略：披露一点信息→收一点钱→再披露一点信息→再收一点钱⋯⋯ 这种交错进行的多轮互动，是无法被一个单-轮机制所模拟的。

3.4 预算约束下的简化

引入预算约束，这个看似简单的现实因素，却极大地简化了最优机制的结构，使得多轮“挤牙膏”式的复杂机制变得不再必要。

其核心思想在于，预算约束限制了支付的可能性。特别是，论文中设计了一种巧妙的支付方式，称为“存款-返还” (Deposit-Return)，它有效地解决了不承诺买方的跑路问题。

咨询机制 (Consulting Mechanism)是一种简洁而强大的机制，是预算约束下信息销售问题的最优解。其一般形式如下：

1. 咨询开始：买方向卖方（顾问）报告自己的私有类型θ。
2. (可选) 存款：在需要时，买方需要先存入一笔押金（通常是其预算上限）。
3. 内部处理：卖方根据买方的报告θ和自己的ω，决定两件事：
   - 一个推荐给买方的最佳行动a^*。
   - 一个支付（或返还）金额。
4. 给出建议并结算：卖方将推荐行动a^*告诉买方，并完成最终的资金结算。

这个机制的巧妙之处在于它的支付规则。它绕过了直接对“信息”定价的难题，转而对“行动建议”收费。并且通过“存款-返还”的结构，即便支付金额依赖于卖方的信息ω，也能保证不承诺的买方不会跑路。

我们将在后续章节详细剖析这种咨询机制是如何通过线性规划来求解的，以及它为何在有预算约束时能达到最优。

4 求解最优机制：从独立信号到咨询机制

本章的目标是，将机制设计问题从一个抽象的“寻找最佳规则”问题，转变为一个具体的、可以求解的线性规划 (Linear Programming, LP) 问题。

4.1 独立信号下的最优机制

我们从最简单但富有启发性的情况开始：

- 买方信号ω和卖方类型θ互相独立，即$\mu(\omega, \theta) = \mu(\omega)\mu(\theta)$。
- 没有预算约束。
- 买方是不承诺的。

根据第三章的定理3.2，我们知道在这种情况下，最优机制一定是单轮的。更具体地说，它是一种“先收费，后披露”的机制，被称为定价映射机制 (Pricing Mappings Mechanism)，这等价于向买方提供一个“合约菜单”。

4.1.1 合约菜单的视角

一个直接显示机制可以被看作是卖方向买方提供一个合约菜单 (Menu of Contracts)$\{(Y_\theta, t_\theta)\}_{\theta \in \Theta}$。

- 菜单上的每一项(Y_θ, t_θ)都是一个“合约”，它名义上是为类型为θ的买方准备的。
- t_θ是购买该合约的价格。
- Y_θ是一个信号生成器。它是一个随机变量，其分布依赖于卖方的真实信息ω。买方购买合约后，卖方会根据ω从Y_θ中抽取一个信号s并发送给买方。

买方的决策过程：

1. 一个真实类型为θ的买方，会审视菜单上的所有合约。
2. 对于每个合约 $(Y_{\theta'}, t_{\theta'})$，他会计算如果自己购买该合约能获得的期望效用。
3. 他会选择那个能给他带来最高净效用的合约。
4. 他还会在“购买最优合约”和“什么都不买”（获得保留效用）之间进行比较。

卖方的设计问题：卖方的目标是设计这个菜单$\{(Y_\theta, t_\theta)\}$，使得：

1. 激励相容 (Incentive Compatibility, IC)：对于每个θ，类型为θ的买方确实觉得合约(Y_θ, t_θ)是菜单上最好的选择（或者之一）。

2. 个体理性 (Individual Rationality, IR)：对于每个θ，类型为θ的买方购买合约(Y_θ, t_θ)的净效用，不低于他不参与交易的保留效用。
3. 在满足以上两个条件下，最大化总期望收益$\sum_\theta \mu(\theta) t_\theta$。

4.1.2 信息的数学表示：从信号到后验

“信号生成器Y_θ”这个概念仍然有些抽象。为了进行数学优化，我们需要一种更具体的方式来描述信息。一个关键的转化是：任何关于信息披露的机制，其本质都是在改变买方的后验信念。

- 一个信号s的全部意义，在于它如何更新买方对ω的信念。
- 在收到信号s之前，买方的信念是先验$p(\omega)$（因为信号独立，先验就是$\mu(\omega)$）。
- 在收到信号s之后，根据贝叶斯法则，买方的信念更新为一个后验分布$q(\omega) = \Pr(\omega|s)$。

因此，我们可以用后验分布的分布来等价地描述一个信号生成器Y_θ:Y_θ不再是生成信号s，而是以一定的概率$x_\theta(q)$，直接生成一个后验分布q。买方支付t_θ后，他会得到一个后验分布q，然后基于这个q去做决策。

如果买方的后验信念是q，他的最优期望效用是：

$$v_\theta(q) = \max_{a \in A} \mathbb{E}_{\omega \sim q}[u(\theta, \omega, a)] = \max_{a \in A} \sum_{\omega \in \Omega} q(\omega) u(\theta, \omega, a)$$

函数$v_\theta(q)$是q的一个分片线性凸函数（它是多个线性函数的最大值）。

一个后验的分布$\{x_\theta(q)\}$并非任意的，它必须满足一个物理约束：所有可能的后验的期望，必须等于先验。这被称为贝叶斯可信性 (Bayesian Plausibility) 或可行性约束 (Feasibility Constraint)。

$$\mathbb{E}_{q \sim x_\theta}[q] = \sum_q x_\theta(q) \cdot = p(\text{其中} p(\omega) = \mu(\omega))$$

这个约束保证了卖方不能“无中生有”地创造信息。

4.1.3 构建线性规划 (LP)

现在，我们可以将所有元素组合起来，构建一个用于求解最优合约菜单的线性规划。

设t_θ为每个买方类型θ设计的价格。$x_\theta(q)$：对于每个类型θ和每个可能的后验q，选择生成后验q的概率。

我们不需要考虑所有可能的后验。因为效用函数$v_\theta(q)$是分片线性的，其“拐点”只发生在有限的位置。我们可以预先计算出一个有限的、足够大的“有趣后验”集合Q^*，最优机制只会从这个集合中选择后验来生成。Q^*的大小是关于$|A|, |\Omega|, |\Theta|$的多项式。这个结论使得变量的数量从无限变成了有限（尽管可能仍然很大）。

线性规划 LP1 (独立信号)

$$
\begin{aligned}
\max_{t,x} \quad & \sum_{\theta\in\Theta} \mu(\theta) t_\theta & & (\text{目标: 最大化期望收益}) \\
\text{s.t.} \quad & \sum_{q\in Q^*} x_\theta(q) v_\theta(q) - t_\theta \geq \sum_{q\in Q^*} x_{\theta'}(q) v_\theta(q) - t_{\theta'} & \forall \theta, \theta' \in \Theta \quad & (\text{IC: 类型}\theta\text{不羡慕}\theta') \\
& \sum_{q\in Q^*} x_\theta(q) v_\theta(q) - t_\theta \geq v_\theta(p) & \forall \theta \in \Theta \quad & (\text{IR: 购买不劣于不买}) \\
& \sum_{q\in Q^*} x_\theta(q) \cdot q = p & \forall \theta \in \Theta \quad & (\text{可行性: 后验的期望是先验}) \\
& \sum_{q\in Q^*} x_\theta(q) = 1 & \forall \theta \in \Theta \quad & (\text{概率和为1}) \\
& x_\theta(q) \geq 0, \quad t_\theta \geq 0 & \forall \theta, q \quad & (\text{非负性})
\end{aligned}
$$

- IC 约束：左边是类型为θ的买方购买合约(Y_θ, t_θ)的净效用，右边是他冒充θ'购买合约$(Y_{\theta'}, t_{\theta'})$的净效用。注意，当他冒充时，他收到的是为$\theta'$设计的信号，但他评估价值时用的是自己的效用函数$v_\theta$。
- IR 约束：购买合约的净效用，不低于他的保留效用$v_\theta(p)$（基于先验p做决策的效用）。
- 可行性约束：保证了信息披露的物理可能性。

这个 LP 的变量数量和约束数量都是关于$|\Theta|$和$|Q^*|$的多项式。虽然$|Q^*|$可能很大，但这个问题原则上是可以在多项式时间内求解的。更妙的是，通过考察其对偶问题 (Dual Problem)，可以利用椭球法 (Ellipsoid Method) 和分离预言机 (Separation Oracle) 在多项式时间内求解，即使$|Q^*|$是指数级的。这证明了最优机制是可计算的。

4.1.4 一个具体的计算例子

让我们回顾第一部分中的代码示例，并用这里的LP框架来分析它。

- $\Theta = \{0, 1\}, \Omega = \{0, 1\}$
- $v_0(q)$和$v_1(q)$是两个关于后验$q(\omega = 1)$的分片线性凸函数。
- $p = (0.5, 0.5)$是先验。
- 我们计算出$\xi(0) = 2.0, \xi(1) = 2.0$。保留效用$v_0(p) = v_1(p) = 2.0$。

一个简单的可行解是：

- 合约菜单：只提供一个合约(Y, t)。
- 价格t：设为2.0。
- 信息披露Y：完全披露ω。这等价于，如果$\omega = 0$，生成的后验是$q = (1, 0)$；如果$\omega = 1$，生成的后验是$q = (0, 1)$。这个Y的可行性：$0.5 \times (1, 0) + 0.5 \times (0, 1) = (0.5, 0.5) = p$，满足。

- 验证约束：
  - IR:对$\theta = 0$，购买后的期望效用是 10.0 (因为总能做出正确决策)，支付 2.0，净效用 8.0。不购买的保留效用也是 8.0。所以 8.0≥8.0 满足。$\theta = 1$同理。
  - IC：因为只有一个合约，IC约束自动满足。
- 收益：$\mu(0) \times t + \mu(1) \times t = 2.0$

这与我们之前通过“密封信封”机制找到的解是一致的。但LP框架更加通用，即使在$\xi(\theta)$不同，或者最优机制需要部分披露信息时，LP依然能找到最优解。

4.2 引入预算约束：咨询机制的诞生

引入一个关键的现实因素：预算约束。

每个买方(θ, b)有一个预算b，他支付的总额不能超过b。为了简化，我们假设预算是公开的（即$\mu(\omega, \theta, b)$中，b是确定的）。私有预算的情况类似，只是增加了对b的激励约束。卖方也有一个预算M，她支付给买方的总额不能超过M。

预算约束如何改变游戏？它使得一种更简洁、更强大的机制成为可能——咨询机制 (Consulting Mechanism)。

定义 4.1 (直接支付的咨询机制, CM-dirP)这是一种非常直观的机制，模拟了真实的咨询过程：

1. 承诺 (Commit): 卖方（顾问）首先公开承诺一套“服务方案”。对于每一种可能的买方报告类型θ，她都定义了：
2. 报告 (Report): 买方（客户）向卖方报告自己的类型θ。
3. 支付 (Pay): 买方支付服务费t_θ。
4. 推荐 (Recommend): 卖方根据真实的ω和买方的报告θ，按照$p_\theta(a|\omega)$随机抽取一个行动a，并将其作为“建议”告诉买方。

“听话”约束 (Obedience Constraint)这种机制有一个至关重要的内在约束，称为听话约束 (Obedience Constraint)。卖方承诺的推荐策略$p_\theta(a|\omega)$必须是“诚实”的，即当买方被推荐了行动a时，他自己计算后发现，a确实是当前情况下的最优选择。

形式化地，当买方被推荐行动a时，他会更新自己对ω的信念。新的后验是$\Pr(\omega|\text{推荐} = a)$。他必须发现，最大化 $\sum_{\omega} \Pr(\omega|\text{推荐} = a)u(\theta, \omega, a')$ 的a'就是a。

$$a = \arg\max_{a' \in A} \sum_{\omega \in \Omega} \mu(\omega) p_\theta(a|\omega) u(\theta, \omega, a')$$

卖方需要设计的东西不再是抽象的“信号生成器”，而是具体的“行动推荐策略”。由于行动集合A通常比后验空间Q^*小得多，这大大简化了设计空间。在有公开预算和独立信号的情况下，这种直接支付的咨询机制 (CM-dirP) 是最优的。

4.2.1 咨询机制的线性规划 (LP)

我们可以为 CM-dirP 构建一个更紧凑、变量更少的线性规划。

设t_θ为类型θ设计的价格。$p_\theta(a|\omega)$推荐策略。为了让它成为 LP 的变量，我们通常定义$z_\theta(a,\omega)=\mu(\omega)p_\theta(a|\omega)$。$\sum_a p_\theta(a|\omega)=1$的约束就变成了$\sum_a z_\theta(a,\omega)=\mu(\omega)$。

线性规划 LP2 (咨询机制)

$$
\begin{aligned}
\max_{t,z} \quad & \sum_{\theta\in\Theta}\mu(\theta)t_\theta \\
\text{s.t.} \quad & \sum_{a,\omega} z_\theta(a,\omega)u(\theta,\omega,a)-t_\theta \ge \sum_{a,\omega} z_{\theta'}(a,\omega)u(\theta,\omega,a)-t_{\theta'} && \forall\theta,\theta' \quad \text{(IC)} \\
& \sum_{a,\omega} z_\theta(a,\omega)u(\theta,\omega,a)-t_\theta \ge v_\theta(p) && \forall\theta \quad \text{(IR)} \\
& \sum_{\omega} z_\theta(a,\omega)u(\theta,\omega,a) \ge \sum_{\omega} z_\theta(a,\omega)u(\theta,\omega,a') && \forall\theta,a,a' \quad \text{(Obedience)} \\
& \sum_{a\in A} z_\theta(a,\omega)=\mu(\omega) && \forall\theta,\omega \quad \text{(可行性)} \\
& t_\theta \le b && \forall\theta \quad \text{(Budget)} \\
& z_\theta(a,\omega)\ge 0, \quad t_\theta\ge 0 && \forall\theta,a,\omega
\end{aligned}
$$

这个 LP 的变量数量是$|\Theta|+|\Theta|\times|A|\times|\Omega|$，约束数量也是这些参数的多项式。这是一个标准大小的LP，可以用任何现成的求解器（如 Gurobi, CPLEX）高效求解。这比之前需要椭球法的 LP1 在实践中要高效得多。

4.2.2 私有预算与存款-返还机制

如果买方的预算b是其私有信息θ的一部分，那么 CM-dirP 就不再最优了。因为买方可能会为了支付更低的服务费t_θ而谎报自己的预算。

存款-返还的咨询机制 (CM-depR)流程：

1. 报告与存款: 买方报告其类型和预算(θ,b)，并立即存入其声称的全部预算b作为押金。
2. 推荐与返还: 卖方根据报告(θ,b)和ω，推荐一个行动a，并返还一笔金额给买方。最终买方支付的净额为$t_{\theta,b}$。净支付额$t_{\theta,b}$是由卖方设计的。返还的金额是$b-t_{\theta,b}$。

“先存后返”的结构，使得买方无法通过谎报来获利。如果他低报预算，比如真实预算是100，他谎报是50，那么他最多只能存50，这会限制他能参与的合约。如果他高报预算，他根本拿不出那么多钱来做押金。这个简单的操作有效地“检验”了买方的预算声明，从而恢复了激励相容性。

CM-depR 是私有预算和独立信号下的最优机制，并且同样可以被一个标准大小的线性规

划求解。

4.3 终极挑战：相关信号与概率性返还

当信号相关时，即使有预算约束，问题也变得更加复杂。买方的支付必须依赖于卖方最终揭示的信息。

一种被称为概率性返还的咨询机制 (CM-probR) 在最一般的情况下（相关信号，私有预算）都是最优的。

机制流程:

1. 报告与存款: 买方报告(θ, b)并存入预算b。
2. 推荐与概率性结果: 卖方根据(θ, b)和ω，随机决定一个组合(a, i)，其中a是推荐行动，i是一个支付结果的指示器，$i \in \{返还0, 返还(b+M)\}$。
3. 如果i是“返还0”，买方净支付b。如果i是“返还$(b+M)$”，卖方向买方支付M，买方净支付$-M$。

这个机制看起来非常奇特，为什么要引入卖方预算M，并且支付额如此极端？

强烈的激励信号：这两种极端的支付结果，向不同类型的买方传递了非常强烈的不同信号。因为信号是相关的，类型为θ和θ'的买方对ω的信念不同，因此他们对“最终支付b”和“最终倒拿M”这两种情况发生的概率预期也不同。利用相关性：卖方正是利用了这种预期的差异，来精细地进行价格歧视，从而榨取最大收益。这呼应了著名的 Cremer-McLean 机制的思想，即当买方类型充分相关时，卖方几乎可以榨取所有剩余价值。

5 关键定理与证明 (Key Theorems and Proofs)

们将严谨地证明，在预算约束下，简洁的咨询机制 (Consulting Mechanism) 能够实现与任何复杂交互协议相同的最优收益。证明的核心是利用线性规划的对偶理论 (Duality Theory)，通过一系列精巧的变换，揭示最优机制的内在结构。

5.1 CM-probR定理

我们将证明的核心定理是 [Chen et al. 2020] 的主要结果，即概率性返还的咨询机制 (CM-probR) 的最优性。这个证明过程也将隐含地证明其他简化情况下的最优性。

我们的证明将遵循之前提到的“三步走”策略：

- **基准确立：** 明最优机制存在于存款-返还的定价结果机制 (POM-depR) 类别中。
- **对偶变换：** 将寻找最优 POM-depR 的问题表述为原始LP P，然后通过$P \to D \to D'$的变换，得到一个变量数可控的对偶LP D'。

- **结构揭示**: 将D'对偶回新的原始LPP'，并证明P'的最优解对应一个 CM-probR 机制。

引理 5.1 (POM-depR 的最优性):对于任何一个能为卖方带来期望收益R的通用交互协议，都存在一个 POM-depR 机制，它能带来至少为R的期望收益。

现在，我们将 POM-depR 的最优化问题转化为一个线性规划，并对其进行变换。为使符号简洁，我们主要讨论公开预算b的情况。私有预算的情况可以通过将(θ, b)视为一个复合类型来处理，分析是类似的。

如前所述，一个信号披露策略可以被等价地描述为对买方先验信念的凸分解 (convex decomposition)。

外部观察者 (Outside Observer): 假设有一个虚拟的外部观察者，他不知道买方的类型θ，他看到的先验是$\mu(\omega)$。

买方: 类型为θ的买方，他看到的先验是$\mu(\omega|\theta)$。

信念转换: 当外部观察者看到后验为q时，类型θ的买方根据贝叶斯法则，看到的后验将是$D_\theta q/(1^T D_\theta q)$，其中$D_\theta$是一个对角矩阵，其对角线元素为$\mu(\theta|\omega)$。

买方价值函数: 类型θ的买方对外部后验q的（未归一化的）价值为$v_\theta(D_\theta q)$，其中$v_\theta(p) = \max_{a\in A} \sum_\omega p(\omega)u(\theta, \omega', a)$。$v_\theta$ 是齐次函数，即

$$v_\theta(c \cdot p) = c \cdot v_\theta(p) \text{ for } c > 0$$

一个 POM-depR 机制由一组(x_θ, t_θ)决定，其中x_θ是一个后验分布，$t_\theta(q)$是对应后验q的价格。我们使用变量$x_\theta(q)$表示选择后验q的概率，$\tau_\theta(q) = x_\theta(q)t_\theta(q)$表示期望支付。

最优 POM-depR 的问题可以写成如下（可能无限维的）线性规划P：

$$\begin{array}{llll}
\max & \displaystyle\sum_{\theta\in\Theta}\sum_{q\in Q^*}\tau_\theta(q) & & \\
\text{s.t.} & \displaystyle\sum_q (v_\theta(D_{\theta'}q)x_\theta(q) - \tau_\theta(q)) - \sum_q (v_\theta(D_{\theta'}q)x_{\theta'}(q) - \tau_{\theta'}(q)) \ge 0 & \forall\theta,\theta' & \text{(IC)} \quad : \lambda_{\theta,\theta'} \\
& \displaystyle\sum_q (v_\theta(D_\theta\mu)x_\theta(q) - \tau_\theta(q)) \ge v_\theta(D_\theta\mu) & \forall\theta & \text{(IR)} \quad : \alpha_\theta \\
& \displaystyle\sum_q x_\theta(q)\cdot q = \mu & \forall\theta & \text{(Feasibility)} \quad : y_\theta \\
& b\cdot x_\theta(q) - \tau_\theta(q) \ge 0 & \forall\theta, q & \text{(Budget)} \quad : \beta_\theta(q) \\
& \tau_\theta(q) + M\cdot x_\theta(q) \ge 0 & \forall\theta, q & \text{(Seller Budget)} \quad : \xi_\theta(q) \\
& x_\theta(q)\ge 0, \beta_\theta(q)\ge 0, \xi_\theta(q)\ge 0 & &
\end{array}$$

这里μ是$\mu(\omega)$的向量形式。Q^*是一个足够大的离散后验集合。在约束的右侧，我们标注了其对应的对偶变量。

我们来推导P的对偶问题D.D的目标是最小化原始问题约束右侧项与对偶变量乘积的和。D的约束来自于对每个原始变量（$x_\theta(q)$和$\tau_\theta(q)$）的系数进行整理。

对于原始变量$\tau_\theta(q)$，其系数必须满足：

$$-\sum_{\theta'\neq\theta}\lambda_{\theta,\theta'}\cdot(-1)-\alpha_\theta\cdot(-1)-\sum_{\theta'\neq\theta}\lambda_{\theta',\theta}\cdot 1-\beta_\theta(q)\cdot(-1)+\xi_\theta(q)\cdot 1\geq 1$$

整理得：

$$1+\sum_{\theta'}\lambda_{\theta',\theta}-\sum_{\theta'}\lambda_{\theta,\theta'}-\alpha_\theta-\beta_\theta(q)-\xi_\theta(q)=0(\text{ 因为'P'是最大化问题})$$

令$\Lambda_\theta=1-\alpha_\theta-\sum_{\theta'\neq\theta}(\lambda_{\theta,\theta'}-\lambda_{\theta',\theta})$，则有$\beta_\theta(q)+\xi_\theta(q)=\Lambda_\theta$。由于$\beta$和$\xi$非负，这意味着$\Lambda_\theta$必须非负，且$\beta$和$\xi$在$\Lambda_\theta$上进行分配。

对于原始变量$x_\theta(q)$，其系数必须满足：

$$\left(v_\theta(D_\theta q)(1-\alpha_\theta-\sum_{\theta'\neq\theta}\lambda_{\theta,\theta'})-\sum_{\theta'\neq\theta}v_{\theta'}(D_\theta q)\lambda_{\theta',\theta}\right)+(y_\theta^T q)+b\cdot\beta_\theta(q)-M\cdot\xi_\theta(q)\geq 0$$

(这里我们暂时忽略$\lambda_{\theta,\theta}$)。

将$\beta_\theta(q)=\Lambda_\theta-\xi_\theta(q)$带入，并重新整理，得到$D$的约束：

$$y_\theta^T q+v_\theta(D_\theta q)\Lambda_\theta^{\text{self}}-\sum_{\theta'\neq\theta}v_{\theta'}(D_\theta q)\lambda_{\theta',\theta}+b\Lambda_\theta-(b+M)\xi_\theta(q)\geq\quad\forall\theta,q$$

其中Λ_θ和$\Lambda_\theta^{\text{self}}$是关于$\alpha,\lambda$的线性表达式。

对偶问题D如下：

$$\begin{aligned}
\min\quad & \sum_\theta v_\theta(D_\theta\mu)\alpha_\theta+y_\theta^T\mu & \\
\text{s.t.}\quad & y_\theta^T q+\cdots-(b+M)\xi_\theta(q)\geq 0 & \forall\theta,q\\
& \Lambda_\theta\geq\xi_\theta(q)\geq 0 & \forall\theta,q\\
& \alpha_\theta,\lambda_{\theta,\theta'}\geq 0 &
\end{aligned}$$

这个对偶问题D仍然有指数多的变量$\xi_\theta(q)$。

引理5.2：对偶问题D的约束可以被等价地替换为一组新的约束，这组新的约束中不再含有变量$\xi_\theta(q)$。

我们来分析D的约束。对于固定的θ,λ,α,y，约束可以写成：

同时我们还有约束$0 \le \xi_\theta(q) \le \Lambda_\theta$。为了使所有约束都成立，我们必须能够为每个$q$找到一个$\xi_\theta(q)$满足上述两个条件。这等价于要求两个上界中较小的一个，必须大于等于下界0.即，对于所有的q：

$$\min\left(\Lambda_\theta, \frac{y_\theta^T q + ...}{b+M}\right) \ge 0$$

由于$b+M>0$和$\Lambda_\theta \ge 0$，这等价于两条独立的约束：

1. $\Lambda_\theta \ge 0$（这条已经隐含在$\xi_\theta(q) \le \Lambda_\theta$和$\xi_\theta(q) \ge 0$中）
2. $y_\theta^T q + \text{terms\_not\_depending\_on\_xi}(q) \ge 0$

现在，让我们回到D约束的原始形式，并观察$\xi_\theta(q)$是如何出现的

$$y_\theta^T q + \text{terms}(\lambda,\alpha) - (b+M)\xi_\theta(q) \ge 0$$

对于给定的λ,α,y，是否存在$\beta_\theta(q)$,$\xi_\theta(q)$使得D的所有约束都满足。

$$\beta_\theta(q) + \xi_\theta(q) = \Lambda_\theta, \quad \beta_\theta(q) \ge 0, \xi_\theta(q) \ge 0$$

将$\beta_\theta(q) = \Lambda_\theta - \xi_\theta(q)$代入。

我们还需要满足$0 \le \xi_\theta(q) \le \Lambda_\theta$。

因此，对于任意q，上述不等式的右侧必须有一个解$\xi_\theta(q)$存在于$[0,\Lambda_\theta]$。（假设$b+M>0$）

这给出了两条关于y,Λ,α的，与ξ无关的约束：

1. $y_\theta^T q - \text{cost\_term}(q) + b\Lambda_\theta \ge 0$
2. $y_\theta^T q - \text{cost\_term}(q) - M\Lambda_\theta \le 0$

将cost_term(q)和Λ_θ展开回λ,α的表达式，我们就得到了一个新的对偶LP D'。

$$\begin{aligned}
\min \quad & \sum_\theta v_\theta(D_\theta\mu)\alpha_\theta + y_\theta^T\mu \\
\text{s.t.} \quad & y_\theta^T q - \left(v_\theta(D_{\theta'}q)\Lambda_\theta^{\text{self}} - \sum_{\theta'\neq\theta} v_{\theta'}(D_\theta q)\lambda_{\theta',\theta}\right) + b\left(1-\alpha_\theta - \sum_{\theta'}(\lambda_{\theta,\theta'} - \lambda_{\theta',\theta})\right) \ge 0 \quad \forall\theta, q \quad : x_\theta^+(q) \\
& y_\theta^T q - \left(v_\theta(D_{\theta'}q)\Lambda_\theta^{\text{self}} - \sum_{\theta'\neq\theta} v_{\theta'}(D_\theta q)\lambda_{\theta',\theta}\right) - M\left(1-\alpha_\theta - \sum_{\theta'}(\lambda_{\theta,\theta'} - \lambda_{\theta',\theta})\right) \le 0 \quad \forall\theta, q \quad : x_\theta^-(q) \\
& \alpha_\theta, \lambda_{\theta,\theta'} \ge 0, y_\theta \in \mathbb{R}^{|\Omega|}
\end{aligned}$$

这个D'只有多项式数量的变量(α,λ,y)，但仍然有指数/无限多的约束(对每个q)。

现在，我们对D'进行对偶操作，得到新的原始LP P'。P'的变量是$x_\theta^+(q)$和$x_\theta^-(q)$，对应D'的两组主要约束。

对D'中每个对偶变量α_θ，$\lambda_{\theta,\theta'}$，y_θ的系数进行整理，可以推导出P'的约束。P'的目标函数则来自D'约束的右侧项（在这里是μ和$v_\theta(D_\theta\mu)$）。经过繁琐但直接的代数运算，我们得到P'的形式：

$$
\begin{aligned}
\max_{\theta,q} \quad & \left(b \cdot x_\theta^+(q) - M \cdot x_\theta^-(q)\right) \\
\text{s.t.} \quad & \sum_q \left((v_\theta(D_\theta q) - b)x_\theta^+(q) + (v_\theta(D_\theta q) + M)x_\theta^-(q)\right) \\
& - \sum_q \left((v_\theta(D_\theta q) - b)x_{\theta'}^+(q) + (v_\theta(D_\theta q) + M)x_{\theta'}^-(q)\right) \geq 0 \qquad \forall \theta, \theta' \quad \text{(IC)} \\
& \sum_q \left((v_\theta(D_\theta q) - b)x_\theta^+(q) + (v_\theta(D_\theta q) + M)x_\theta^-(q)\right) \geq v_\theta(D_\theta \mu) \qquad \forall \theta \quad \text{(IR)} \\
& \sum_q (x_\theta^+(q) + x_\theta^-(q)) \cdot q = \mu \qquad \forall \theta \quad \text{(Feasibility)} \\
& x_\theta^+(q) \geq 0, x_\theta^-(q) \geq 0
\end{aligned}
$$

P'的目标函数和约束完美地诠释了一个机制：

- 当买方报告θ时，以总概率$\sum_q x_\theta^+(q)$要求支付净额b。
- 当买方报告θ时，以总概率$\sum_q x_\theta^-(q)$要求支付净额$-M$。
- 信息披露策略由后验分布$\{x_\theta^+(q), x_\theta^-(q)\}$描述。

我们需要证明P'存在一个最优解，其中信息披露等价于行动推荐。

引理5.3：线性规划P'存在一个最优解$\{x_\theta^+, x_\theta^-\}$，使得对于任意$\theta$和任意支付结果 $o \in \{+, -\}$，集合$\{q | x_\theta^o(q) > 0\}$，每一个$q$都对应一个不同的、由$\arg\max_a v_\theta(D_\theta q)$ 决定的最优行动。

假设我们有一个最优解x^*不满足这个型中。即，存在θ, o和两个不同的后验q_1, q_2，使得$x_\theta^{o*}(q_1) > 0, x_\theta^{o*}(q_2) > 0$，并且：

$$
\arg\max_a v_\theta(D_\theta q_1) = \arg\max_a v_\theta(D_\theta q_2) = a^*
$$

现在，我们构造一个新的解x_{new}。令$w_1 = x_\theta^{o*}(q_1)$和$w_2 = x_\theta^{o*}(q_2)$。定义一个新的后验$q_{\text{new}} = \frac{w_1 q_1 + w_2 q_2}{w_1 + w_2}$。在$x_{\text{new}}$中，我们将$q_1$和$q_2$的概率清零，并将它们的总概率$w_1 + w_2$赋给$q_{\text{new}}$：

- $x_{\theta,new}^o(q_1) = 0$
- $x_{\theta,new}^o(q_2) = 0$
- $x_{\theta,new}^o(q_{new}) = w_1 + w_2$
- 所有其它的x值保持不变。

我们需要验证x_{new}仍然是P'的一个可行解，并且目标函数值不变。

1. 目标函数值: 目标函数只依赖于x的总和，与q的具体分布无关，因此目标值不变。
2. 可行性约束:
$$\sum_q \left(x_\theta^+(q) + x_\theta^-(q)\right) \cdot q = \mu$$
新解在这一项的改变量是$(w_1+w_2)q_{new} - (w_1q_1+w_2q_2) = 0$。所以可行性约束仍然满足。
3. IC/IR 约束: 约束的每一项都是形如$\sum_q f(q)x(q)$的求和。我们需要证明，这个合并操作不会使得任何约束的左侧项变得更小（从而可能违反$\geq$约束）。核心在于$v_\theta(D_\theta q)$函数的性质。因为a^*同时是q_1和q_2的最优行动，这意味着$v_\theta(D_\theta q)$在q_1和q_2之间的连线上是线性的。
$$v_\theta(D_\theta q_{new}) = v_\theta\left(D_\theta \frac{w_1q_1+w_2q_2}{w_1+w_2}\right) = \frac{w_1v_\theta(D_\theta q_1) + w_2v_\theta(D_\theta q_2)}{w_1+w_2}$$
这个线性关系保证了所有约束项的值在合并前后保持不变。对于其他类型的买方$\theta' \neq \theta, v_{\theta'}(D_{\theta'}q)$不一定在$q_1$和$q_2$之间是线性的，但它一定是凸的。
$$v_{\theta'} \leq \frac{w_1v_{\theta'}(D_{\theta'}q_1) + w_2v_{\theta'}(D_{\theta'}q_2)}{w_1+w_2}$$
这个凸性关系意味着，对于其他买方的IC约束（即当他们谎报成θ时），合并后的新解给他们带来的效用不会增加，因此如果原约束满足，新约束也一定满足。

通过这个构造性的“合并”证明，我们表明总能找到一个最优解，其中每个后验都对应一个唯一的行动推荐。此时，披露后验q等价于推荐行动a。这正是 CM-probR 机制的定义。

由于强对偶性，P'的最优值等于P的最优值。我们证明了最优的 POM-depR 的收益，可以被一个 CM-probR 机制达到。再结合引理 5.1，我们最终得出结论：CM-probR 是所有可能机制中的最优机制。

证毕!

5.2 机制的稳健性：最优收益的连续性分析

在前面的部分，我们都假设上下文(u,μ)是精确已知且固定的。然而在实践中，卖方对联合分布μ的估计可能存在误差。一个自然且重要的问题是：如果真实的上下文(u',μ')与卖方所设想的(u,μ)非常接近，那么最优收益$R(u',\mu')$是否也与$R(u,\mu)$相近？换言之，最优收益函数R否是连续的？

在最一般的情况下（允许负支付），最优收益函数$R(u,\mu)$不是连续的，但它是下半连续的 (Lower Semicontinuous)。如果我们对机制施加一些“合理”的限制，比如不允许卖方向买方支付（即无正转移），或者机制是更简单的定价映射机制，那么最优收益函数就是连续的 (Continuous)。

我们将重点证明其中最核心、最微妙的部分：最优收益函数$R(u,\mu)$的下半连续性。

设$C = \mathbb{R}^{|\Theta|\times|\Omega|\times|A|} \times \Delta(\Theta\times\omega)$为所有可能上下文 (u,μ)构成的空间，赋予其标准的欧几里得拓扑。最优收益函数$R : C \to \mathbb{R}$。

一个函数$f : X \to \mathbb{R}$在点x是下半连续的，如果对于任意收敛到x的点列$\{x_n\}$，都有：

$$f(x) \leq \lim_{n\to\inf} \inf f(x_n)$$

直观上讲，这意味着x_n趋近于x时，函数值$f(x_n)$不会发生“向下的突然跳跃”。它可以“向上跳”，但不能“向下跳”。

我们的目标是证明：对于任意上下文$c = (u,\mu)$，以及任意收敛到c的上下文序列$c_n = (u_n,\mu_n)$，我们有$R(u,\mu) \leq \lim\inf_{n\to\inf} R(u_n,\mu_n)$。

证明的关键在于，我们需要展示对于c的最优（或近似最优）机制，当上下文从c稍微扰动到c_n时，这个机制仍然是“近似可行的”，并且其收益也只是发生了微小的变化。

根据前面的分析，我们知道最优机制存在于 POM-depR类别中。一个定价结果机制可以被一个元组$M = (\{x_\theta\},\{\tau_\theta\})$所完全描述，其中： x_θ是一个后验空间$\Delta(\Omega)$上的概率测度(probability measure)，满足

$$\int_{q\in\Delta(\Omega)} q dx_\theta(q) = \mu$$

（这里的μ 指$\mu(\omega)$分布。）τ_θ是一个$\Delta(\Omega)$上的带号测度 (signed measure)，代表支付。

我们将机制空间M看作是所有满足可行性、IC和IR约束的这种测度元组的集合。这里的后验空间$\Delta(\Omega)$ 是一个紧致的度量空间。测度空间（如x_θ所在的$M(\Delta(\Omega))$）的拓扑结构需要小心处理。我们赋予它*弱-拓扑。

在泛函分析中，对于一个紧致空间K，其上的概率测度空间$P(K)$弱-*拓扑下也是紧致的（根据 Banach-Alaoglu 定理）。弱-*拓扑下的收敛$\mu_n \to \mu$意味着，对于所有连续函数$f : K \to \mathbb{R}$，都有：

$$\int_K f d\mu_n \to \int_K f d\mu$$

这个拓扑结构非常适合我们的问题，因为所有的效用和支付的期望值，都可以表示为对某个连续函数（如$v_\theta(D_\theta q)$）的极分。

直接处理带等号的 IC/IR 约束很麻烦，因为当上下文c发生微小变化时，原本成立的等式可能就不成立了。我们需要一个更强的结论：

引理5.4（严格偏好机制）对于任意上下文$c = (u,\mu)$和任意$\epsilon > 0$，存在一个定价结果机制M^*，它能产生收益$R(M^*) \geq (1-\epsilon)R(u,\mu)$并且在该机制下，所有的 IC 和 IR 约束都以严格不等式成立（除非两个合约完全相同）。

假设我们有一个最优机制M_{opt}，其收益为$R(u,\mu)$。考虑一个新的机制M^*，它的信息披露策略 x^*_θ与M_{opt}完全相同，但其支付$\tau^*_\theta(q)$是原支付的$(1-\epsilon)$倍，即$\tau^*_\theta(q) = (1-\epsilon)\tau_\theta(q)$。

新机制的收益是$(1-\epsilon)R(u,\mu)$。

让我们检查IC约束：

$$\sum_q (v_\theta(D_\theta q)x_\theta(q) - (1-\epsilon)\tau_\theta(q)) \geq \sum_q (v_\theta(D_{\theta'} q)x_{\theta'}(q) - (1-\epsilon)\tau_{\theta'}(q))$$

将$(1-\epsilon)$提出，这等价于：

$$\sum_q v_\theta(D_\theta q)x_\theta(q) - \sum_q v_\theta(D_{\theta'} q)x_{\theta'}(q) \geq (1-\epsilon)\left(\sum_q \tau_\theta(q) - \sum_q \tau_{\theta'}(q)\right)$$

而在原始机制M_{opt}中，IC 约束要求：

$$\sum_q v_\theta(D_\theta q)x_\theta(q) - \sum_q v_\theta(D_{\theta'} q)x_{\theta'}(q) \geq \sum_q \tau_\theta(q) - \sum_q \tau_{\theta'}(q)$$

比较这两条，如果原始约束是严格大于，新约束在ϵ足够小时也成立。如果原始约束是严格等于，那么只有当$\sum \tau_\theta > 0$时，新约束才可能被违反。但可以证明，这种情况可以通过调整消除。最终，我们可以构造出一个所有约束都严格成立的机制，其收益任意接近最优收益。

现在我们来完成下半连续性的证明。令$c_n = (u_n, \mu_n)$是一个收敛到$c = (u, \mu)$的上下文序列。我们的目标是证明$R(c) \leq \liminf R(c_n)$。

根据引理 5.4，对于任意给定的$\epsilon > 0$，我们可以在上下文c下找到一个机制M_ϵ，它的收益$R(M_\epsilon) \geq (1-\epsilon)R(c)$，并且其所有的IC和IR约束都是严格大于。

一个机制$M = (\{x_\theta\}, \{\tau_\theta\})$的可行性（即 IC, IR, Feasibility 约束的满足）可以被看作是一个对应 (correspondence) $F : C \rightrightarrows \mathcal{M}$，它将每个上下文$c$映射到所有在该上下文下可行的机制集合$F(c)$。

- IC 约束形如：

$$\int v_\theta(D_\theta q)dx_\theta - \int d\tau_\theta - \left(\int v_\theta(D_{\theta'} q)dx_{\theta'} - \int d\tau_{\theta'}\right) \geq 0$$

- 所有的v_θ, D_θ 都连续地依赖于上下文c。
- 这意味着，约束函数是机制M和上下文c的一个联合连续函数。

考虑我们找到的机制M_ϵ。由于它的所有约束都是严格成立的，根据连续性，当上下文从c稍微扰动到c_n时（当n足够大时），这些约束仍然会成立。这意味着，对于所有足够大的n，机制M_ϵ在上下文c_n下也是一个可行的机制。

形式化地，因为约束函数$g(c, M)$是连续的，且$g(c, M_\epsilon) > 0$，那么存在一个c的邻域$N(c)$，使得对于所有$c' \in N(c)$，都有$g(c', M_\epsilon) > 0$。因为$c_n \to c$，所以当n足够大时，$c_n \in N(c)$。

因此，对于所有足够大的n，我们有：

$$R(c_n) = \sup_{M \in F(c_n)} \text{Revenue}(c_n, M) \geq \text{Revenue}(c_n, M_\epsilon)$$

$R(c_n)$是在c_n下的最优收益，它必然不低于任何一个可行机制（如M_ϵ）的收益。

现在我们取下极限：

$$\lim_{n \to \inf} \inf R(c_n) \geq \text{Revenue}(c, M_\epsilon)$$

根据M_ϵ的构造，我们有$\text{Revenue}(c, M_\epsilon) = R(M_\epsilon) \geq (1 - \epsilon) R(c)$。所以：

$$\lim_{n \to \inf} \inf R(c_n) \geq (1 - \epsilon) R(c)$$

这个不等式对任意的$\epsilon > 0$都成立。因此，我们可以令$\epsilon \to 0$，得到最终的结论：

$$\lim_{n \to \inf} \inf R(c_n) \geq R(c)$$

这正是下半连续性的定义。

证毕!