

2026–2027 学年短学期

课程综合实践 II：数据要素交易基础

Lec 07: 拍卖与机制设计基础（二）

吴一航 yhwu_is@zju.edu.cn

浙江大学计算机科学与技术学院



CONTENT

目录

1. 福利最大化机制

2. 迈尔森最优机制

3. 数据定价与不完全信息

接下来开始讨论福利最大化和卖家利润最大化拍卖机制设计，首先考虑福利最大化目标，卖家利润最大化将在下一节介绍。

接下来开始讨论福利最大化和卖家利润最大化拍卖机制设计，首先考虑福利最大化目标，卖家利润最大化将在下一节介绍。

此前已经知道，单物品第二价格拍卖可以实现福利最大化；

- 因为每个理性竞拍者都会如实报告自己的估值，物品将分配给报价最高（也就是估值最高）的竞拍者，从而实现福利最大化；
- 当然我们的目标不止于此，本节希望将福利最大化机制推广到更一般的拍卖或物品分配等场景。

考虑一般的物品分配场景：

- 例如有两个竞拍者和四个不同的物品（例如四个不同地区/不同频段的频谱），记为 $S = \{A, B, C, D\}$ ；
- 买家长对 S 的任意子集都有不同的估值；
- 可能的分配结果 Ω 包含将所有物品分配出去的所有可能结果，其中 $\omega \in \Omega$ 表示一个合理的分配结果；
 - 例如将 B 分配给竞拍者 1， A, C, D 分配给竞拍者 2 就是一个合理的分配结果。

如何为这种情况设计福利最大化的拍卖机制？

考虑一般的物品分配场景：

- 例如有两个竞拍者和四个不同的物品（例如四个不同地区/不同频段的频谱），记为 $S = \{A, B, C, D\}$ ；
- 买家对 S 的任意子集都有不同的估值；
- 可能的分配结果 Ω 包含将所有物品分配出去的所有可能结果，其中 $\omega \in \Omega$ 表示一个合理的分配结果；
 - 例如将 B 分配给竞拍者 1， A, C, D 分配给竞拍者 2 就是一个合理的分配结果。

如何为这种情况设计福利最大化的拍卖机制？

自然地，读者可能会想到迈尔森引理，然而最大的困难是，迈尔森引理中买家对物品的估值是一维变量可以描述的，此处无法做到。事实上迈尔森引理至今无法在推广到多维的一般情况下有类似于一维情形的简洁刻画。

因此我们需要求助于其他的机制。记可能的分配结果集合记为 Ω ，其中 $\omega \in \Omega$ 表示一个合理的分配结果。下面首先假设所有竞拍者是诚实报价的，即对分配结果 ω 的报价 $b_i(\omega)$ 就等于他对 ω 中给他分配的物品的效用值，则下面的分配规则给出了福利最大化的分配规则：

$$\omega^* = \arg \max_{\omega \in \Omega} \sum_{i=1}^n b_i(\omega).$$

因此我们需要求助于其他的机制。记可能的分配结果集合记为 Ω ，其中 $\omega \in \Omega$ 表示一个合理的分配结果。下面首先假设所有竞拍者是诚实报价的，即对分配结果 ω 的报价 $b_i(\omega)$ 就等于他对 ω 中给他分配的物品的效用值，则下面的分配规则给出了福利最大化的分配规则：

$$\omega^* = \arg \max_{\omega \in \Omega} \sum_{i=1}^n b_i(\omega).$$

此外，为了讨论方便，记 ω_{-i}^* 为去掉参与人 i 后的福利最大化分配结果，即 $\omega_{-i}^* = \arg \max_{\omega \in \Omega} \sum_{j \neq i} b_j(\omega)$ 。记所有参与人的投标向量为 $\mathbf{b} = (b_1, \dots, b_n)$ ，下面的支付公式给出了福利最大化 DSIC 机制的支付规则：

$$p_i(\mathbf{b}) = \sum_{j \neq i} b_j(\omega_{-i}^*) - \sum_{j \neq i} b_j(\omega^*).$$

上述公式的含义是， i 需要支付的价格是，在 i 不参与分配时其他人的最大福利减去 i 参与分配时最大福利情况下其他人的福利。事实上也可以视为参与人 i 给其他参与人带来的外部性。

结合以上的分配规则和支付规则，就得到了一般物品分配场景下的福利最大化 DSIC 机制，称之为**维克里-克拉克-格罗夫斯（Vickrey-Clarke-Groves）**机制，或简称 **VCG 机制**。

值得一提的是，VCG 机制是由三位依次对这一机制的提出做出贡献的经济学家的名字命名的：

- 其中的第一位，威廉·维克里（William Vickrey）是 1996 年诺贝尔经济学奖得主，可惜的是在获奖后三天在去开会的路上去世；
 - 维克里首次提出并证明了第二价格拍卖的诚实性，因此第二价格拍卖也被称为维克里拍卖；
- 上述支付公式则是由克拉克于 1971 年提出的，因此实际上这一机制应当被称作**克拉克机制（Clarke mechanism）**，或称**主角机制（pivot mechanism）**；
- 而后格罗夫斯在 1973 年给出了 VCG 机制更一般的形式。

事实上，二价拍卖是 VCG 机制在单物品拍卖下的特例：

- 首先分配机制满足福利最大化，这在单物品拍卖中就是将物品分配至对物品估值最高的竞拍者，因此与二价拍卖一致；

事实上，二价拍卖是 VCG 机制在单物品拍卖下的特例：

- 首先分配机制满足福利最大化，这在单物品拍卖中就是将物品分配至对物品估值最高的竞拍者，因此与二价拍卖一致；
- 其次是支付规则：
 - 如果你不是估值最高的，那么你不参与时的最大福利等于估值最高的竞拍者的估值 v_i ，你参与时的最大福利也等于估值最高的竞拍者的估值 v_i ，并且此时你的福利等于 0，因此支付等于 $v_i - (v_i - 0) = 0$ ；

事实上，二价拍卖是 VCG 机制在单物品拍卖下的特例：

- 首先分配机制满足福利最大化，这在单物品拍卖中就是将物品分配至对物品估值最高的竞拍者，因此与二价拍卖一致；
- 其次是支付规则：
 - 如果你不是估值最高的，那么你不参与时的最大福利等于估值最高的竞拍者的估值 v_i ，你参与时的最大福利也等于估值最高的竞拍者的估值 v_i ，并且此时你的福利等于 0，因此支付等于 $v_i - (v_i - 0) = 0$ ；
 - 如果你是估值最高的，那么你不参与时的最大福利等于估值第二高的竞拍者的估值 v_j ，你参与的情况下的最大福利等于你的估值 v ，并且此时你的福利等于 v ，因此支付等于 $v_j - (v - v) = v_j$ ；
 - 由此可以看出 VCG 的支付规则也与二价拍卖一致。

第一个需要介绍的性质是 DSIC，即诚实报价占优。定理的证明略去，只需要知道这一结论即可：

定理

VCG 机制是 DSIC 的。

第一个需要介绍的性质是 DSIC，即诚实报价占优。定理的证明略去，只需要知道这一结论即可：

定理

VCG 机制是 DSIC 的。

在 DSIC 的基础上，VCG 满足的第二个性质是使得社会福利最大化，因为 VCG 机制在保证诚实报价的情况下基于报价实现了福利最大化的分配。这一性质也被称为**事后有效率**，即事后阶段也能满足福利最大化。类似地也可以定义事前、事中角度的期望福利最大化；

- VCG 机制不依赖于任何先验分布假设，因此不讨论事前、事中效用；

第一个需要介绍的性质是 DSIC，即诚实报价占优。定理的证明略去，只需要知道这一结论即可：

定理

VCG 机制是 DSIC 的。

在 DSIC 的基础上，VCG 满足的第二个性质是使得社会福利最大化，因为 VCG 机制在保证诚实报价的情况下基于报价实现了福利最大化的分配。这一性质也被称为**事后有效率**，即事后阶段也能满足福利最大化。类似地也可以定义事前、事中角度的期望福利最大化；

- VCG 机制不依赖于任何先验分布假设，因此不讨论事前、事中效用；

第三个性质是，在 VCG 机制下，每个参与人的支付必定是大于等于 0 的，这也就避免了出现拍卖中支付小于 0 的不正常情况；

- 回忆支付公式，减号前对应除 i 之外的参与人的最大福利，减号后对应的只是除 i 之外的参与人的某种可能的福利，因此减号后的值必定小于等于减号前的值，从而保证了支付的非负性。

第四个性质涉及到一个新的概念，即**个人理性 (individual rationality)**，通常简称为 IR：

- 个人理性指所有参与人参与机制产生的效用都不会低于其不参与机制时的效用。通常不参与机制的效用为 0，因此个人理性的定义可以简化为所有参与人的效用都不会低于 0；
- 相应的，个人理性也有事前、事中和事后的版本，分别对应事前、事中期望效用大于等于 0 以及事后的实际效用大于等于 0；
- 这一性质称为个人理性也是不难理解的，因为如果一个参与人的效用低于 0，那么他就没有参与机制的动机，因此机制设计者应当保证所有参与人的效用都不会低于 0，这样理性的参与人才会选择参与机制。

下面需要说明 VCG 机制满足事后个人理性。不难写出参与 VCG 机制的事后效用满足

$$\begin{aligned} u_i &= b_i(\omega^*) - p_i(\mathbf{b}) \\ &= \sum_{i=1}^n b_i(\omega^*) - \sum_{j \neq i} b_j(\omega_{-i}^*) \\ &\geq 0 \end{aligned}$$

不等号成立是显然的：前者是 n 人最大福利，后者是其中部分人的最大福利。

接下来则要开始讨论 VCG 机制的缺陷，从两个例子入手讨论：

例

第一个例子考虑一般的多物品拍卖：假设有 n 个竞拍者， m 个物品，则有效的分配结果集合 Ω 为所有 n 个竞拍者对 m 个物品的分配方式，有 n^m 种可能的分配结果。对于每个竞拍者 i ，只要他们报告对每个 $\omega \in \Omega$ 的估值，就可以根据 VCG 机制的分配和支付规则计算出分配结果和支付结果。

接下来则要开始讨论 VCG 机制的缺陷，从两个例子入手讨论：

例

第一个例子考虑一般的多物品拍卖：假设有 n 个竞拍者， m 个物品，则有效的分配结果集合 Ω 为所有 n 个竞拍者对 m 个物品的分配方式，有 n^m 种可能的分配结果。对于每个竞拍者 i ，只要他们报告对每个 $\omega \in \Omega$ 的估值，就可以根据 VCG 机制的分配和支付规则计算出分配结果和支付结果。

由此可以看出 VCG 机制非常强大，只要设计好可行的分配机制集合 Ω ，并且有参与人对任意的 $\omega \in \Omega$ 的估值，就可以得到福利最大化的 DSIC 机制。但转念一想，如果 m 和 n 的数量很大时，每个参与人需要报告相当巨大数量的估值，并且求解福利最大化问题也是指数级别的复杂度，因此 VCG 机制在很多实际场景中并不适用，还需要研究其它组合拍卖机制。

通过这个例子，我们理解了 VCG 虽然能解决非常一般化的问题，但具有计算困难性，因此在现实中并不常用。

第二个例子请同学们尝试从计算结果中得到启发：

例

考虑有三个竞拍者两个物品 A 和 B 的多物品拍卖：

- 第一个竞拍者对同时获得两个物品有估值 1（即 $v_1(AB) = 1$ ），其余情况均为 0；
- 第二个竞拍者只对赢得物品 A 有估值 1，即 $v_2(A) = v_2(AB) = 1$ ，其余情况均为 0；
- 第三个竞拍者只对赢得物品 B 有估值 1，即 $v_3(B) = v_3(AB) = 1$ ，其余情况均为 0。

回答下面两个问题：

1. 计算只有前两个竞拍者时和三个竞拍者全在时的 VCG 机制的结果；
2. 你能从中总结出什么？增加竞拍者会减少单物品二价拍卖的收益吗？

CONTENT

目录

1. 福利最大化机制

2. 迈尔森最优机制

3. 数据定价与不完全信息

本节从卖家收益的角度考虑拍卖机制设计问题，即**如何设计一个使得卖家的收益最大化的拍卖机制**，又称最优机制；

- 最优机制这一名称来源于其诞生的论文，即诺贝尔经济学奖得主迈尔森于 1981 年发表的著名论文 *Optimal auction design*；
- 可以说这篇论文是理论经济学最伟大的论文之一，开创了一套完整的理论范式，后续无数文章都使用了本文提出的技术解决问题；
- 本质而言这篇文章从理论上完美解决了参与人私人信息是一维变量的情况下，利润的最大化机制设计问题，给出了显式解；
 - 参与人私人信息是高维变量的情况至今只有一些特殊情况的解，一般情况的最优机制显式解仍然是公开问题；
- 这一部分证明虽然有趣且有价值，但技术性较强，故我们只简要介绍结果，具体证明不展开，感兴趣的同学可以阅读原论文。

考虑单物品情况，即一个卖家有一个不可分割的物品待出售；

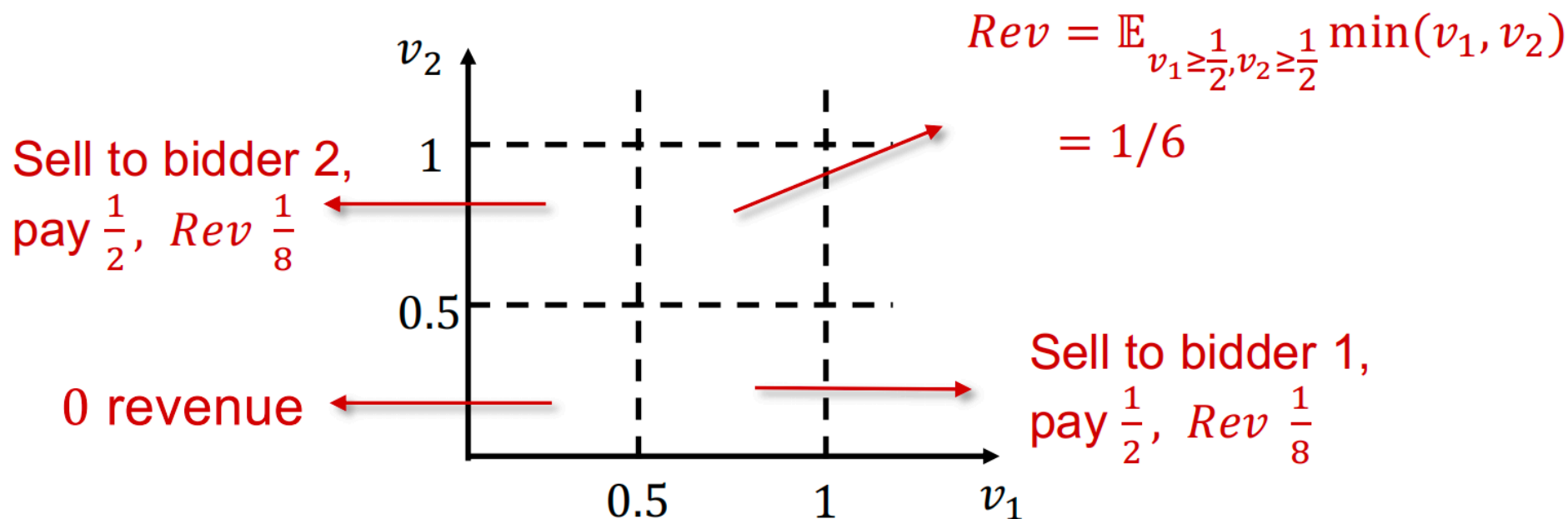
- 与此前单物品讨论一致，有 n 个潜在买家（竞拍者） $N = \{1, 2, \dots, n\}$ ；
- 每个买家 i 对物品有一个心理价位 t_i 是不完全信息；
 - 其连续先验概率密度 $f_i : [a_i, b_i] \rightarrow \mathbb{R}^+$ 是共同知识，且 $f_i(t_i) > 0$ 对所有 $t_i \in [a_i, b_i]$ 成立；
- 假定不同买家的估值分布是相互独立的（但不需要同分布）。

例

考虑有两个买家估值独立且均服从 $[0, 1]$ 上的均匀分布的情况，假设此时采用保留价格为 $1/2$ 的第二价格拍卖，求卖家的收益。

例

考虑有两个买家估值独立且均服从 $[0, 1]$ 上的均匀分布的情况，假设此时采用保留价格为 $1/2$ 的第二价格拍卖，求卖家的收益。



问题：比较没有保留价格的结论，你发现了什么？为什么保留价格机制能打破收入等价原理的限制，获得更高的收益？

对每个买家 $i \in N$ ，记 $c_i(t_i) = t_i - \frac{1-F_i(t_i)}{f_i(t_i)}$ 为虚拟估值。若 $c_i(t_i)$ 关于 t_i 是单调递增的（即满足正则化条件，大部分常见分布均满足这一条件）。迈尔森证明了如下结论：

- 最优机制的分配规则是：将物品分配给虚拟估值最大的买家 i ，且要求 $c_i(t_i) \geq 0$ （若有多个满足条件则按概率抽取）；
- 最优机制的支付规则是（根据迈尔森引理）：买家 i 的支付为 $p_i(t) = z_i(t_{-i})x_i(t)$ ，其中 x_i 是分配规则，且

$$z_i(t_{-i}) = \inf\{s_i \mid c_i(s_i) \geq 0 \text{ 且 } c_i(s_i) \geq c_j(t_j), \forall j \neq i\}$$

即 $z_i(t_{-i})$ 是使得参与人 i 刚好能有机会获得物品的最低报价。如果只有一个 i 满足 $c_i(t_i) \geq 0$ 和 $c_i(t_i) \geq c_j(t_j), \forall j \neq i$ ，则 $x_i(t) = 1$ ，且

$$p_i(t) = \begin{cases} z_i(t_{-i}), & x_i(t) = 1 \\ 0, & x_i(t) = 0. \end{cases}$$

考虑一种最简单的情况来具象化前面给出的结论。考虑一个所有买家估值独立同分布的情形（即对称模型），并且符合正则化条件，不难得到

$$z_i(t_{-i}) = \max \left\{ c^{-1}(0), \max_{j \neq i} t_j \right\}.$$

考虑一种最简单的情况来具象化前面给出的结论。考虑一个所有买家估值独立同分布的情形（即对称模型），并且符合正则化条件，不难得到

$$z_i(t_{-i}) = \max \left\{ c^{-1}(0), \max_{j \neq i} t_j \right\}.$$

- 结合前面得到的 (x, p) ，此时的**最优机制其实就是一个含保留价格的二价拍卖机制，其中保留价格为 $c^{-1}(0)$** ；
- 因为此时所有买家估值同分布，因此虚拟估值函数也相同，故具有最高估值（最高报价）的赢得物品，并且支付第二高报价和保留价格之间的较高者，并且如果最高报价低于保留价格，则不分配物品。

更具体而言，当所有买家估值独立且服从 $[0, 1]$ 上的均匀分布时，虚拟估值函数为 $c_i(t_i) = 2t_i - 1$ ，因此保留价格为 $1/2$ ，此时的最优机制就是保留价格为 $1/2$ 的第二价格拍卖，这正是前面给出的例子研究的机制。

限于课时与难度，我们下面只给出证明的大致思路：

1. **利用显示原理将机制设计空间限制在直接显示机制**，因此只需要设计竞拍者如实报告估值的机制，因此卖家收益最大化问题可以写为如下数学规划问题：

$$\begin{aligned} \max_{\mathbf{x}, \mathbf{p}} \quad & U_0 = \int_T \left(\sum_{i=1}^n p_i(t) \right) f(t) \, dt \\ \text{s.t.} \quad & (\mathbf{x}, \mathbf{p}) \text{ 满足 BIC,} \\ & (\mathbf{x}, \mathbf{p}) \text{ 满足个人理性,} \\ & \sum_{i=1}^n x_i(t) \leq 1. \end{aligned}$$

2. 利用 BIC 迈尔森引理将 BIC 转化为两个更易于处理的等价条件；
3. 将个人理性条件转化为更易于处理的等价条件；
4. 将目标函数利用积分变换等，将目标问题转化为虚拟福利最大化问题并求解。

第 2 - 4 步实际上就是将数学规划的约束和目标函数变得更加清晰，从而可以在下一节中给出显示的最大化解。

- 事实上很多问题的本质都是数学规划问题，但**最优机制问题具有特殊的结构从而可以给出很漂亮的显式解**，这些特殊结构的发现就是迈尔森这篇文章最大的贡献，并且这一结构在很多问题上都有出现，因此在未来非常多的工作中都应用了迈尔森这一套方法；
- 本质上很多问题都可以表达为数学规划问题，解决问题的方式就是找到特殊结构（例如背包问题动态规划），但现实中很多问题无法找到内在的特殊结构。

尽管最优机制可以使得卖家获得最大的期望收益，但是这一机制存在一些天然的缺陷：

1. **卖家很难准确估计每一个买家的估值分布**，因此这一机制很难完美实现，特别是应用于数据拍卖场景时，数据买家的估值不确定性更大，因此之后会讨论在无先验分布下的机制设计；

尽管最优机制可以使得卖家获得最大的期望收益，但是这一机制存在一些天然的缺陷：

1. **卖家很难准确估计每一个买家的估值分布**，因此这一机制很难完美实现，特别是应用于数据拍卖场景时，数据买家的估值不确定性更大，因此之后会讨论在无先验分布下的机制设计；
2. 非对称模型（即买家的估值不同分布）下，**报价最高的买家可能并不是最有可能获得物品的买家**。这一点非常显然，因为不同的分布下 c 的形态会有所不同；
 - 若 $f_i(t_i) = \frac{1}{b_i - a_i}$ ，即买家的估值均匀分布，不难计算得到 $c_i(t_i) = 2t_i - b_i$ ，这关于 t_i 是单调递增的，因此符合正则化条件；
 - 但是此时的最优机制是选出 $2t_i - b_i$ 最大的 i ，如果 $b_i < b_j$ ，那么可能存在 $t_i < t_j$ 但是 $2t_i - b_i > 2t_j - b_j$ 的情况，即报价更低的买家可能获得物品；

3. 最优机制不是事后有效率的，例如我们考虑对称模型下，卖家估值等于 0 且买家估值都大于 0 的情况，此时显然物品要售出才是福利最大化（也是帕累托最优或事后有效率）的，但是如果所有买家的报价都低于 $c_i^{-1}(0)$ ，那么物品就不会被售出，这显然不是事后有效率的。

3. 最优机制不是事后有效率的，例如我们考虑对称模型下，卖家估值等于 0 且买家估值都大于 0 的情况，此时**显然物品要售出才是福利最大化（也是帕累托最优或事后有效率）的，但是如果所有买家的报价都低于 $c_i^{-1}(0)$ ，那么物品就不会被售出，这显然不是事后有效率的。**

当然最优机制仍然是具有实际意义的：雅虎曾在广告拍卖中加入保留价格，发现了保留价格的确能带来利润提升——这就是理论研究指导实践的意义所在。

3. 最优机制不是事后有效率的，例如我们考虑对称模型下，卖家估值等于 0 且买家估值都大于 0 的情况，此时**显然物品要售出才是福利最大化（也是帕累托最优或事后有效率）的，但是如果所有买家的报价都低于 $c_i^{-1}(0)$ ，那么物品就不会被售出，这显然不是事后有效率的。**

当然最优机制仍然是具有实际意义的：雅虎曾在广告拍卖中加入保留价格，发现了保留价格的确能带来利润提升——这就是理论研究指导实践的意义所在。

最后需要提醒的一点是，如果是**单位需求下多个相同物品的拍卖，只有分配规范性条件会改变，其余推导均没有任何变化：**

- 问题：假设买家具具有单位需求（每个买家只需要一个物品），那么此时最大化利润的拍卖规则是什么；
- 因此最优机制**可以直接应用于已知买家估值先验分布的数据拍卖中。**

CONTENT

目录

1. 福利最大化机制

2. 迈尔森最优机制

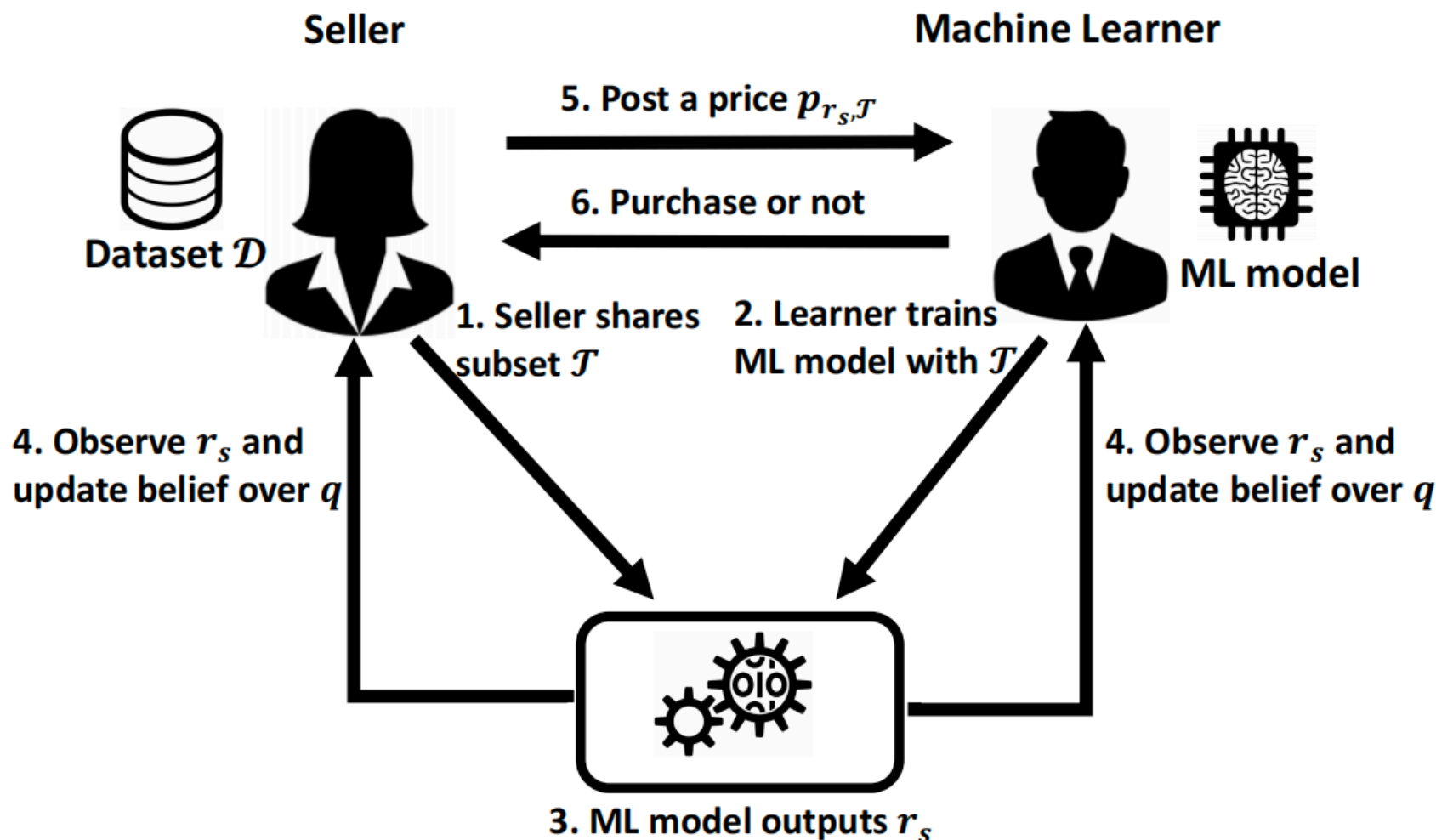
3. 数据定价与不完全信息

接下来将介绍数据定价的基本策略。这些基本策略主要针对数据的两大特性：（1）零成本复制；（2）价值不确定性。下一讲的版本化定价是针对零成本复制的特性，本节将介绍针对数据价值不确定的定价策略。数据价值不确定性主要分为如下两个角度：

1. **卖家不确定数据对于买家的价值**：例如卖家不知道买家购买数据的下游任务等。针对这一角度，诚实的**拍卖机制**可以显示买家对数据的真实估值，而**多臂老虎机算法**对于不确定性问题的天然优势，可以解决卖家不确定数据对买家的价值情况下的定价问题；
2. **买家本身也不确定数据对自身的价值**：例如买家在购买数据前很难判断数据对于自身目标任务的价值等。针对这一角度将有**数据免费试用策略**，通过免费试用数据可以让数据买家（甚至数据卖家）更了解数据对买家任务的价值，获得更合理的定价结果。

多臂老虎机算法应用于数据定价的相关文献大都模型简单但技术性很强，感兴趣的读者可以阅读教材相关内容了解。这里仅介绍数据免费试用策略和拍卖数据定价的基本思想。

核心思想：通过免费试用数据使得买家对数据价值估计更为准确，但免费试用也使得免费部分无法再出售，因此需要权衡免费试用的收益和损失。



针对数据卖家未知数据买家对数据产品估值的问题，拍卖理论中关于设计机制使得买家诚实报出自己的估值的讨论，打破了信息不对称，自然成为了一个合适的解决方案：

- 此前讨论的**最优机制可以很轻松地推广到多个相同物品的情况**，因此在已知各数据买家估值先验分布的情况下的最优机制（利润最大化）设计是可以被迈尔森最优机制直接解决的；
- **福利最大化机制设计则可以根据 VCG 机制解决**；
- 因此研究基于拍卖的数据定价需要挖掘更贴合数据产品本身特性的问题以及现有理论无法解决的非平凡问题。

考虑如下机器学习模型出售场景：

- 数据卖家是零售商店，他们将匿名化的分钟级消费者流量数据流出售到市场中，而数据买家则是希望获得能够预测未来库存需求的物流公司；
- 零售商选择使用拍卖的形式出售由这些数据训练出的库存需求预测模型，因此需要每个物流公司提供一个报价；

考虑如下机器学习模型出售场景：

- 数据卖家是零售商店，他们将匿名化的分钟级消费者流量数据流出售到市场中，而数据买家则是希望获得能够预测未来库存需求的物流公司；
- 零售商选择使用拍卖的形式出售由这些数据训练出的库存需求预测模型，因此需要每个物流公司提供一个报价；
 - 自然地，在机器学习模型出售的场景中，**每个物流公司的报价应当是模型预测单位（1%）准确度提升对其带来的效用增益（将一单位准确率类比为一单位物品）**；
 - 例如，根据物流公司内部测算得知，超出或低于销售量 10% 的备货成本为 10000 元，则物流公司对于每 1% 的库存需求预测准确性提高的估值为 1000 元，这也就是物流公司诚实报价时应当给出的报价。

考虑如下机器学习模型出售场景：

- 数据卖家是零售商店，他们将匿名化的分钟级消费者流量数据流出售到市场中，而数据买家则是希望获得能够预测未来库存需求的物流公司；
- 零售商选择使用拍卖的形式出售由这些数据训练出的库存需求预测模型，因此需要每个物流公司提供一个报价；
 - 自然地，在机器学习模型出售的场景中，**每个物流公司的报价应当是模型预测单位（1%）准确度提升对其带来的效用增益（将一单位准确率类比为一单位物品）**；
 - 例如，根据物流公司内部测算得知，超出或低于销售量 10% 的备货成本为 10000 元，则物流公司对于每 1% 的库存需求预测准确性提高的估值为 1000 元，这也就是物流公司诚实报价时应当给出的报价。

因此接下来的问题便是，如何设计一个拍卖机制使得物流公司愿意诚实报价。回忆上一讲的讨论，只需要为拍卖设计分配机制 x 和支付机制 p 。由于这一拍卖形式只需要要求买家报告一个估值，因此迈尔森引理给出了这一拍卖机制是 DSIC（即买家诚实报价）的充要条件。

迈尔森引理

一个拍卖机制是 DSIC（占优策略激励相容）的，当且仅当其分配规则和支付规则 (x, p) 满足：

- x 是单调的，即 $x_i(b_i)$ 是 b_i 的单调不减函数；
- 给定 x 的情况下，只要给定 $p_i(0)$ 的值，对任意的 $i \in N$ 和 $b_i \in [0, +\infty)$ ， p 的表达式是唯一确定的：

$$p_i(b_i) = p_i(0) + b_i \cdot x_i(b_i) - \int_0^{b_i} x_i(s) \, ds.$$

- 模型可以零成本复制，故分配规则不存在 $\sum_i x_i(b_i) \leq 1$ 的要求；

迈尔森引理

一个拍卖机制是 DSIC（占优策略激励相容）的，当且仅当其分配规则和支付规则 (x, p) 满足：

- x 是单调的，即 $x_i(b_i)$ 是 b_i 的单调不减函数；
- 给定 x 的情况下，只要给定 $p_i(0)$ 的值，对任意的 $i \in N$ 和 $b_i \in [0, +\infty)$ ， p 的表达式是唯一确定的：

$$p_i(b_i) = p_i(0) + b_i \cdot x_i(b_i) - \int_0^{b_i} x_i(s) \, ds.$$

- 模型可以零成本复制，故分配规则不存在 $\sum_i x_i(b_i) \leq 1$ 的要求；
- 买家 i 对模型的报价 b_i 代表其对每 1% 的模型准确度的估值，因此**每个买家能分配到的 $x_i(b_i) \in [0, 1]$ 应当代表模型的准确率**；
 - 这也是出售机器学习模型的拍卖设计相较于普通商品的一大不同：普通商品不可分割且不可零成本复制，分配结果 $x_i(b_i)$ 只能表示获得物品的概率，而**机器学习模型的准确率则自然是一个 $[0, 1]$ 中的常数**，故此时的 $x_i(b_i)$ 可以代表模型的优劣而非获得模型的概率。

总结：

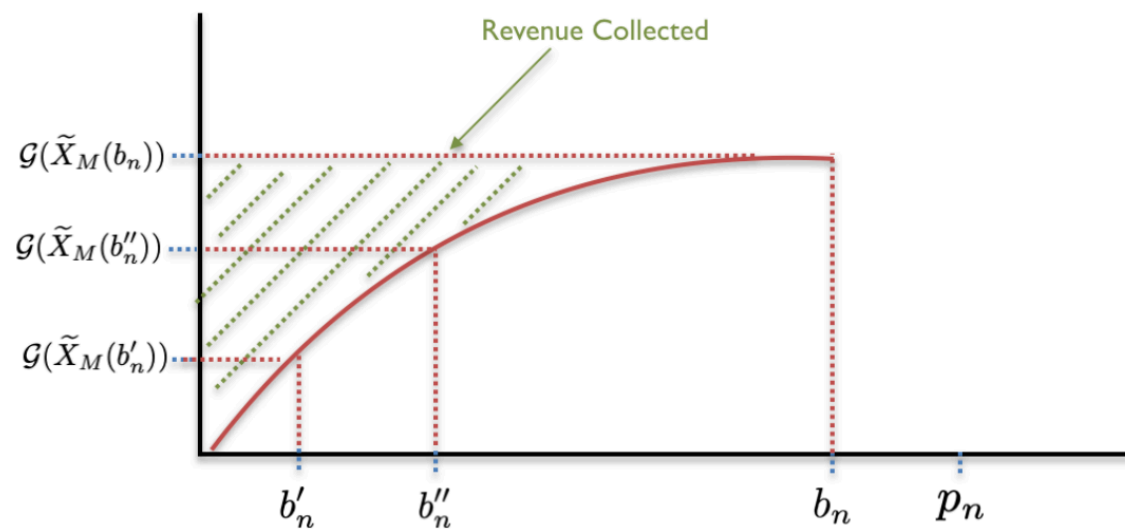
参数	普通商品	机器学习模型
b_i	对单个商品的估值	对单位预测准确度的估值
$x_i(b_i)$	获得物品的概率	模型预测准确率

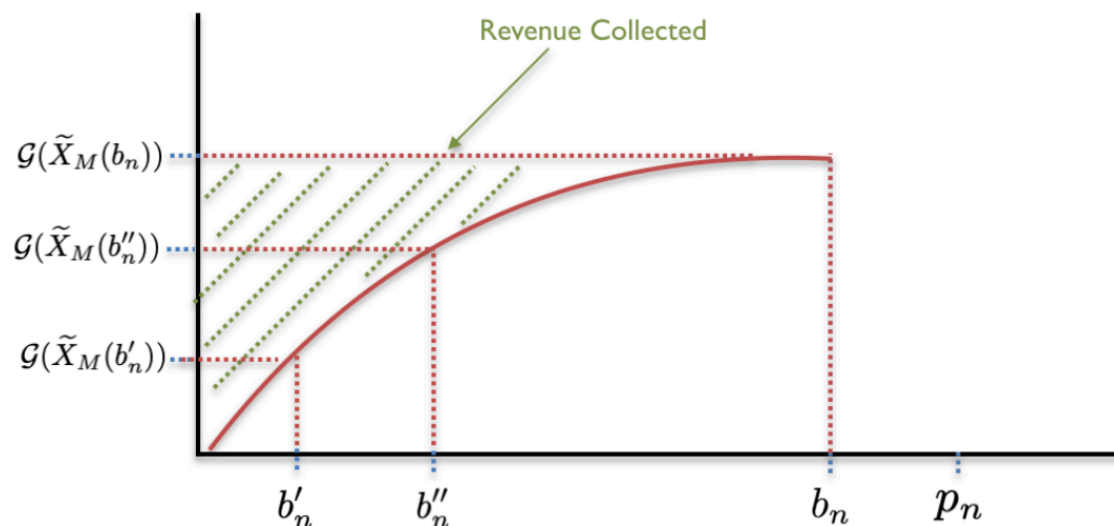
总结：

参数	普通商品	机器学习模型
b_i	对单个商品的估值	对单位预测准确度的估值
$x_i(b_i)$	获得物品的概率	模型预测准确率

下面需要设计机制满足迈尔森引理的条件：

- $x_i(b_i)$ 的单调性要求：一个简单且自然的方案是，首先使用全部数据进行训练获得一个最优模型，并为这一模型设定一个基准价格 q ；
 - 当报价 $b_i \geq q$ 时，则直接出售最优模型；
 - 当 $b_i < q$ 时，则出售添加噪声的模型，并且 b_i 越低添加的噪声越多；
 - 例如假设最优模型输出为 x ，报价为 b_i 时出售的模型输出为 $x + \max(0, q - b_i) \cdot N(0, \sigma^2)$ 即可满足条件。
- 根据单调函数 $x_i(b_i)$ 即可利用迈尔森支付公式决定买家 i 的支付。





问题：基准价格 q 应当如何决定。根据迈尔森支付公式（设 $p_i(0) = 0$ ），由于 q 是一个候选参数且能影响到 x_i 的值，迈尔森支付公式可重写为

$$p_i(b_i, q) = b_i \cdot x_i(b_i, q) - \int_0^{b_i} x_i(s, q) \, ds.$$

如果数据卖家对买家的估值有先验分布，则可以根据先验分布选取最大化支付的 q 。而对于无先验分布的情况，则可以使用此前介绍的乘性权重算法，将买家视为逐个到达的对抗性老虎机，对所有可能的 q 的选择根据乘性权重算法更新每一步的选择概率即可得到一个无憾算法。

注：这一部分只需理解大致思想，具体内容选择这一部分对应的大作业的同学可以进一步理解

假设卖家拥有一份可无限复制但不可分割的数据（此时数据不是上一小节中可任意操纵的机器学习模型，而是一个不可分割的数据集，或者一个在线数字产品例如电影、电子书等），每个买家具具有单位需求（即愿意购买一份数据）。迈尔森最优拍卖假定对买家估值有先验分布，但**没有先验分布时应当如何设计机制？**

注：这一部分只需理解大致思想，具体内容选择这一部分对应的大作业的同学可以进一步理解

假设卖家拥有一份可无限复制但不可分割的数据（此时数据不是上一小节中可任意操纵的机器学习模型，而是一个不可分割的数据集，或者一个在线数字产品例如电影、电子书等），每个买家具具有单位需求（即愿意购买一份数据）。迈尔森最优拍卖假定对买家估值有先验分布，但**没有先验分布时应当如何设计机制**？

- 一个简单的想法是，**考虑所有人的投标独立同分布的情况，此时当买家足够多时 ($n \rightarrow \infty$)，可以通过大量样本学习出投标人估值的分布**；
 - 格里汶科（Glivenko-Cantelli）定理：经验分布函数能够很好地拟合总体分布，所以自然可以由样本来推断总体。

注：这一部分只需理解大致思想，具体内容选择这一部分对应的大作业的同学可以进一步理解

假设卖家拥有一份可无限复制但不可分割的数据（此时数据不是上一小节中可任意操纵的机器学习模型，而是一个不可分割的数据集，或者一个在线数字产品例如电影、电子书等），每个买家具具有单位需求（即愿意购买一份数据）。迈尔森最优拍卖假定对买家估值有先验分布，但**没有先验分布时应当如何设计机制**？

- 一个简单的想法是，**考虑所有人的投标独立同分布的情况，此时当买家足够多时 ($n \rightarrow \infty$)，可以通过大量样本学习出投标人估值的分布**；
 - 格里汶科（Glivenko-Cantelli）定理：经验分布函数能够很好地拟合总体分布，所以自然可以由样本来推断总体。
- DOP 机制：**使用其他 $n - 1$ 个人的报价决定剩余一个人的价格**；
 - 每个人的报价与自己面对的价格无关，故是 DSIC 的；
 - 然而这一拍卖的收益在不满足独立同分布的极端情况下可以任意差。

有 n 个买家，其中 $\frac{n}{b}$ 的买家投标为 $b \gg 1$ ，其余买家投标均为 1：

- 最优固定价格只可能是 1 或 b ，为什么？
- 因此此时最优固定价格为 1 或 b ，收益均为 n 。

然而，当使用 DOP 时：

有 n 个买家，其中 $\frac{n}{b}$ 的买家投标为 $b \gg 1$ ，其余买家投标均为 1：

- 最优固定价格只可能是 1 或 b ，为什么？
- 因此此时最优固定价格为 1 或 b ，收益均为 n 。

然而，当使用 DOP 时：

- 对于一个报价为 1 的买家 i ，如果取价格为 1，则对其余 $n - 1$ 个人的收益为 $n - 1$ ，如果取价格为 b ，则对其余 $n - 1$ 个人的收益为 n ，因此对这一买家应当选择固定价格 b ；

有 n 个买家，其中 $\frac{n}{b}$ 的买家投标为 $b \gg 1$ ，其余买家投标均为 1：

- 最优固定价格只可能是 1 或 b ，为什么？
- 因此此时最优固定价格为 1 或 b ，收益均为 n 。

然而，当使用 DOP 时：

- 对于一个报价为 1 的买家 i ，如果取价格为 1，则对其余 $n - 1$ 个人的收益为 $n - 1$ ，如果取价格为 b ，则对其余 $n - 1$ 个人的收益为 n ，因此对这一买家应当选择固定价格 b ；
- 对于一个报价为 b 的买家 i ，如果取价格为 1，则对其余 $n - 1$ 个人的收益为 $n - 1$ ，如果取价格为 b ，则对其余 $n - 1$ 个人的收益为 $(\frac{n}{b} - 1) \cdot b = n - b$ ，因此对这一买家应当选择固定价格 1。

综上可知，DOP 带来的收益仅为 $\frac{n}{b}$ ，因为只能对 $\frac{n}{b}$ 个报价为 b 的买家收取 1 的价格。由于 b 可以任意大，因此 DOP 可以任意差。

上述例子中已经体现了一个思想：将无先验拍卖机制的收益与固定价格的最优收益进行比较；

- 这是因为无先验拍卖在无先验的情况下实现卖家收益最大化是非常困难的，因为对买家的估值情况一无所知，这一问题似乎无法下手；
- 因此需要转换研究思路，一个可行的方案是将得到最优机制的目标转化为与一些合适的标准进行比较，一个可行的标准就是最优固定价格（实际有一些细微的差别，感兴趣的同学可以阅读大作业给出的参考文献）；
- 称竞争比为最优固定价格下的收益与某一无先验拍卖机制的收益的比值，因此上述 DOP 机制不存在常数竞争比。

上述例子中已经体现了一个思想：将无先验拍卖机制的收益与固定价格的最优收益进行比较；

- 这是因为无先验拍卖在无先验的情况下实现卖家收益最大化是非常困难的，因为对买家的估值情况一无所知，这一问题似乎无法下手；
- 因此需要转换研究思路，一个可行的方案是将得到最优机制的目标转化为与一些合适的标准进行比较，一个可行的标准就是最优固定价格（实际有一些细微的差别，感兴趣的同学可以阅读大作业给出的参考文献）；
- 称竞争比为最优固定价格下的收益与某一无先验拍卖机制的收益的比值，因此上述 DOP 机制不存在常数竞争比。

关于竞争比分析，有如下结论：

- 不存在确定性拍卖是有竞争力的，因此应当考虑随机拍卖机制；
- 不存在竞争比低于 2.42 的拍卖。进一步地，这一下界是紧的，即存在竞争比等于 2.42 的拍卖；
 - 这一结论的前半部分不存在性在 2004 年给出；
 - 后半部分则作为 2004 年论文的一个猜想被给出，而后经过 10 年的等待被证明。

在 RSOP 中，通过随机采样的方式抽取出对每个竞拍者使用最优固定价格的**投标者**，这一随机性的添加使得最差情况的出现概率降低，从而获得具有有限竞争比的拍卖。RSOP 的定义如下：

定义

随机采样最优价格拍卖（random sampling optimal price auction, RSOP）定义如下：

- 将投标向量 $\mathbf{b}$ 均匀随机地分成两个子集：对于每个买家的投标，都以 $\frac{1}{2}$ 的概率随机落入两个子集 $\mathbf{b}'$ 和 $\mathbf{b}''$ 之一；
- 令 $p' = \text{opt}(\mathbf{b}')$, $p'' = \text{opt}(\mathbf{b}'')$ ($\text{opt}(\mathbf{b})$ 为针对 $\mathbf{b}$ 的最优固定价格)；
- 对 $\mathbf{b}''$ 中的投标使用 p' 作为阈值（即 $\mathbf{b}''$ 中低于 p' 的投标被拒绝，投标大于等于 p' 的投标人获得物品并支付 p' ），对 $\mathbf{b}'$ 中的投标使用 p'' 作为阈值。

本节将结合差分隐私的概念进一步讨论近似最优的机制。将差分隐私和机制设计联系在一起的**关键是将差分隐私的定义和机制设计中的诚实性的概念联系起来**。考虑机制设计的诚实性要求，如果所有人诚实汇报，记机制 M 收到的汇报向量为

$$t = (t_1, \dots, t_n)$$

如果参与人 i 偏离诚实汇报，则此时机制收到的汇报向量为

$$t' = (t_1, \dots, t_i', \dots, t_n)$$

诚实性要求，参与人 i 的效用 $u(M(t)) \geq u(M(t'))$ 。

本节将结合差分隐私的概念进一步讨论近似最优的机制。将差分隐私和机制设计联系在一起的**关键是将差分隐私的定义和机制设计中的诚实性的概念联系起来**。考虑机制设计的诚实性要求，如果所有人诚实汇报，记机制 M 收到的汇报向量为

$$t = (t_1, \dots, t_n)$$

如果参与人 i 偏离诚实汇报，则此时机制收到的汇报向量为

$$t' = (t_1, \dots, t_i', \dots, t_n)$$

诚实性要求，参与人 i 的效用 $u(M(t)) \geq u(M(t'))$ 。

一个重要的观察是， t 和 t' 可以视为相邻数据库，机制 M 也可以视为在由参与人汇报向量组成的数据库上执行的查询算法，查询结果为机制的输出结果，因此也可以定义差分隐私性，此时差分隐私的含义为无法从机制给出的结果看出参与人的汇报。

如果 M 满足 ε -差分隐私，根据差分隐私后处理性质（即在满足差分隐私的算法上复合一个与数据库内容无关的函数仍然满足差分隐私性），对定义在机制所有可能结果上的任意的非负效用函数 u ，都有

$$\begin{aligned}\mathbb{E}[u(M(t_i, t_{-i}))] &= \sum_i \Pr(u(M(t_i, t_{-i})) = u_i) \cdot u_i \\ &\leq \sum_i \exp(\varepsilon) \Pr(u(M(t_i', t_{-i})) = u_i) \cdot u_i \\ &= \exp(\varepsilon) \mathbb{E}[u(M(t_i', t_{-i}))],\end{aligned}$$

同理可得

$$\mathbb{E}[u(M(t_i', t_{-i}))] \leq \exp(\varepsilon) \mathbb{E}[u(M(t_i, t_{-i}))]$$

即如果机制 M 满足差分隐私的要求，则参与人偏离诚实报价带来的收益也是有限的，即满足近似诚实性。

下面考虑结合差分隐私设计近似最优的机制。众所周知，差分隐私中最常用的是拉普拉斯机制，然而这一机制在实现利润最大化时存在问题：

例

假设有很多个（大于 4 个）苹果等待出售，有 4 个买家，他们认为苹果的价值分别为 1 元、1 元、1 元和 4.01 元。显然最优定价为 4.01 元，但这一结果可能会导致估值 4.01 元的买家隐私泄漏，故通过差分隐私机制来保护数据买家的隐私，对输出的价格添加噪声。然而拉普拉斯噪声有相等的概率使得最终价格偏高或偏低，一旦偏高（4.02 元），所有买家都不会购买苹果，卖家会损失全部收益，这一结果显然不可接受。

因此需要设计新的差分隐私机制，即指数机制。为了定义指数机制，首先记在数据库 D 上查询结果为 r 时带给查询者的效用为 $u(D, r)$ 。此外需要定义效用函数敏感度

$$\Delta u = \max_r \max_{D_1, D_2} |u(D_1, r) - u(D_2, r)|,$$

r 取遍所有可能的查询结果（这一集合记为 R ）， D_1, D_2 是相邻数据库。

因此需要设计新的差分隐私机制，即指数机制。为了定义指数机制，首先记在数据库 D 上查询结果为 r 时带给查询者的效用为 $u(D, r)$ 。此外需要定义效用函数敏感度

$$\Delta u = \max_r \max_{D_1, D_2} |u(D_1, r) - u(D_2, r)|,$$

r 取遍所有可能的查询结果（这一集合记为 R ）， D_1, D_2 是相邻数据库。

基于此可以定义指数机制如下：

定义

设 D 是数据库， R 是查询结果的集合， $u(D, r)$ 是效用函数， ε 是差分隐私参数，则指数机制 $M_E(D, u, R)$ 以正比于 $\exp\left(\frac{\varepsilon u(D, r)}{2\Delta u}\right)$ 的概率返回任意的结果 $r \in R$ 。

正比于的含义是，上述概率还需要做归一化处理。

不难看出指数机制的设计思路是，给定数据库 D 和效用函数 $u(D, r)$ ，返回的结果 r 的概率与其效用成正相关。也就是说，效用越高的结果被返回的概率越大。

- 回到卖苹果的例子，显然返回最优结果 4.01 元的概率最大，而大于 4.01 的价格带来的效用为 0，因此被返回的概率比较小。
- 可以证明，指数机制 M_E 是 $(\epsilon, 0)$ -差分隐私的。

不难看出指数机制的设计思路是，给定数据库 D 和效用函数 $u(D, r)$ ，返回的结果 r 的概率与其效用成正相关。也就是说，效用越高的结果被返回的概率越大。

- 回到卖苹果的例子，显然返回最优结果 4.01 元的概率最大，而大于 4.01 的价格带来的效用为 0，因此被返回的概率比较小。
- 可以证明，指数机制 M_E 是 $(\varepsilon, 0)$ -差分隐私的。

指数机制可以在保证隐私性、近似诚实性的情况下，满足近似有效率性：定义 $R_{\text{OPT}} = \{r \in R \mid u(D, r) = \text{OPT}_u(D)\}$ ，其中 D 是一个数据库， $\text{OPT}_u(D)$ 表示效用函数为 u 时数据库 D 能返回的效用最大的结果对应的效用值，因此 R_{OPT} 的含义是所有可能的最优查询结果。有如下定理：

定理

给定数据库 D 、效用函数 u 和查询结果集合 R ，对一个满足 ε -差分隐私的指数机制 $M_E(D, u, R)$ 有

$$\Pr \left[u(M_E(D, u, R)) \leq \text{OPT}_u(D) - \frac{2\Delta u}{\varepsilon} \left(\ln \left(\frac{|R|}{|R_{\text{OPT}}|} \right) + t \right) \right] \leq e^{-t}.$$