1 Введение

Одной из основных причин рассмотрения классов игр со случайными параметрами является то, что это хороший метод для изучения этих классов в их полноте и понимания относительной важности различных свойств игр (таких как одновременные или чередующиеся ходы, различные предположения относительно доступа к информации и т.д.)

Ситуация, когда для данной игры заранее может быть известен только её тип, но не её параметры, является типичной при использовании теоретико-игрового подхода к изучению поведения встроенных систем, т.е. когда по крайней мере некоторые из игроков являются программами, а параметры не полностью контролируются. Повышенная частота взаимодействия, которая обычно превышает любую мыслимую способность человека-игрока, и быстрая эволюция параметров взаимодействия делают использование вероятностных методов вполне естественным.

В данной работе мы представляем первые результаты, полученные с помощью этого подхода, применённого к булевым играм [11, 10, 7, 3]. Точнее, мы ограничиваем наше исследование булевыми играми со случайными формулами, представляющими функции выигрыша. Эта модель естественным образом связана с ситуацией, когда рассматриваются игры между автоматизированными системами (например, встроенными системами в компьютерных сетях). Действительно, предполагая, что игроки являются конечными недетерминированными машинами, они могут быть смоделированы семейством булевых формул.

Прежде чем начать исследование, необходимо сделать несколько выборов относительно вероятностной модели.

Относительно элементарных событий: мы выбрали булевы функции как элементарные события. Другим возможным выбором было бы рассмотрение формул как синтаксических объектов, но первый выбор упрощает определение распределений вероятностей, которые естественным образом связаны со свойствами соответствующих булевых игр (в то время как последний выбор потребовал бы справиться со сложным поведением логической эквивалентности формул).

Представляется естественным также рассматривать вероятностное пространство для каждого n, где n — число переменных. Действительно, n является одним из ключевых параметров при рассмотрении сложности булевых функций, и если нам потребуется рассмотреть различные значения n, возможно каким-то образом объединить пространства, построенные для каждого n.

Напомним некоторые базовые свойства булевых функций.

(i) Областью определения этих функций является $\mathbf{2}^n = \{\mathrm{false}, \mathrm{true}\}^n$, множество всех булевых векторов длины n (которое содержит 2^n элементов).

(ii) Каждая булева функция может быть отождествлена с характеристической функцией подмножества $\mathbf{2}^n$ и, таким образом, с самим подмножеством, так что множество всех элементарных событий есть $\Omega = \mathbf{2}^{\mathbf{2}^n}$.

(iii) Подмножество $\mathbf{2}^n$ может быть отождествлено с формулой от n переменных в полной дизъюнктивной нормальной форме[2], которая удовлетворяется в точности этими векторами (каждому вектору соответствует конъюнкция переменных и их отрицаний: true на i-м месте соответствует v_i, а false соответствует $\neg v_i$).

(iv) Множество Ω является полной булевой алгеброй, и логические операторы на элементах Ω соответствуют теоретико-множественным операторам на $\mathbf{2}^n$. Верхним элементом этой алгебры является множество $\mathbf{2}^n \in \Omega$ (оно представляет булеву функцию true), а нижним элементом этой алгебры является множество $\emptyset \in \Omega$ (оно представляет булеву функцию false). То, как эти логические операторы "взаимодействуют" с вероятностью на Ω, является отдельным вопросом, например, $\mathbb{P}(\mathrm{true})$ не обязательно должно быть равно 1.

(v) Существует естественный частичный порядок на элементах Ω, который определяется включением подмножеств $\mathbf{2}^n$ и одновременно булевой импликацией (см. Определение 1 ниже).

Поскольку элементы Ω могут рассматриваться одновременно как булевы функции и как множества булевых векторов, мы предлагаем следующее определение:

Определение 1

Пусть ω_1, ω_2 — две булевы функции ($\omega_1, \omega_2 \in \Omega := \mathbf{2}^{2^n}$). Мы будем писать $\omega_1 \Rightarrow_0 \omega_2$ и говорить, что "ω_2 истинна на ω_1", если для каждого вектора $v \in \mathbf{2}^n$, $\omega_1(v) = \mathrm{true}$ влечёт $\omega_2(v) = \mathrm{true}$. Также это эквивалентно включению ω_1 в ω_2, рассматриваемых как подмножества $\mathbf{2}^n$:

$$\forall \omega_1, \omega_2 \in \mathbf{2}^{2^n}. (\omega_1 \Rightarrow_0 \omega_2) \Leftrightarrow (\omega_1 \subseteq \omega_2).$$

Замечание

Мы можем рассматривать случайные булевы функции как (не обязательно независимые) векторы из 2^n случайных переменных со значениями в $\mathbf{2} = \{\mathrm{false}, \mathrm{true}\}$.

Относительно сигма-алгебры событий: как обычно для конечных вероятностных пространств, мы рассматриваем сигма-алгебру $\mathcal{S}$ всех подмножеств Ω:

$$\mathcal{S} = \mathbf{2}^{2^{2^n}}.$$

Относительно распределений вероятностей на пространствах булевых формул: как отмечено в [8], часто предполагается, что все булевы функции от данного числа переменных имеют одинаковую вероятность (см. также [16]). В данной работе, где мы начинаем наше исследование, мы решили рассмотреть немного более общий класс распределений вероятностей, где булевы функции генерируются схемой Бернулли на булевых векторах с любой вероятностью p в качестве параметра. Некоторые более сложные способы определения распределений вероятностей на булевых выражениях обсуждаются в [8], и мы планируем исследовать их в ближайшем будущем.

В Разделе 2 мы доказываем несколько общих результатов о вероятности выигрышных стратегий, предполагая произвольное распределение вероятностей. Затем в Разделе 3 мы изучаем случай булевых функций, построенных через конечный процесс Бернулли, специализируем наши результаты в этой более простой постановке, затем обсуждаем значимость этих результатов. В Разделе 4 мы дополнительно изучаем вероятность существования выигрышной стратегии для игрока A при новом предположении, что игрок A знает s битов противника. Затем в Разделе 5 мы изучаем скорость роста вышеупомянутой вероятности относительно знания выборов второго игрока. Раздел 6 посвящен техническим замечаниям о формализации наших результатов в помощнике для формальных доказательств Coq [5]. Наконец, обсуждение понятия "негарантированного выигрыша" и его связи с порядком ходов представлено в Приложении A.

Все результаты работы были формально проверены в Coq.[3]

Код Coq доступен онлайн по адресу https://github.com/erikmd/coq-bool-games и также был архивирован, см. [14].

Помимо того факта, что формальная сертификация сама по себе интересна для сообщества TYPES, она в настоящее время является обычной практикой при разработке и характеризации поведения автономных программ, что является одним из предметов данного исследования.

Я сделаю перевод этого математического текста, сохраняя научную точность и форматирование.

2 Вероятность выигрышных стратегий

Основываясь на материале предыдущего раздела, мы можем рассмотреть любую вероятность $\mathbb{P}$, определенную на сигма-алгебре $\mathcal{S} = 2^{2^n}$, и таким образом получить вероятностное пространство $(\Omega, \mathcal{S}, \mathbb{P})$. В этом разделе мы покажем, что в данном контексте можно вывести несколько результатов, какими бы общими они ни казались.

► Пример 2 (использующий Определение 1). Вероятность события "ω истинно на ω_0", с фиксированным $\omega_0 \in \Omega$, равна

$$\mathbb{P}(\omega_0 \Rightarrow_0 \omega) = \sum_{\substack{\omega \\ \omega_0 \Rightarrow_0 \omega}} \mathbb{P}(\{\omega\}).$$

Далее мы рассмотрим Булевы Игры двух игроков A и B со случайной булевой функцией F от n переменных как функцией выигрыша игрока A, и её отрицанием как функцией выигрыша для B. Мы будем предполагать, что A контролирует первые k переменных, а B оставшиеся $n - k$ переменных.

Стратегия игрока A - это любой вектор, принадлежащий 2^k (оценка первых k переменных), а стратегия игрока B - любая оценка оставшихся $n - k$ переменных (вектор из 2^{n-k}).

Исход игры определяется функцией выигрыша игрока A: $F : 2^n \to 2$, которая может рассматриваться как функция $F : 2^k \times 2^{n-k} \to 2$ (отображающая профиль стратегии в булево значение). В продолжении статьи мы будем отождествлять эти два возможных типа для функции F - хотя в формальном описании они будут закодированы соответственно как (bool_fun n) и (bool_game n k).

► Определение 3 (winA). Для любой игры $F : 2^k \times 2^{n-k} \to 2$, стратегия $a = (a_1, \ldots, a_k)$ игрока A является выигрышной, если она выигрывает против любой стратегии $b \in 2^{n-k}$ игрока B:

$$\mathrm{win}_A[F](a) := \forall b \in 2^{n-k}.\, F(a, b) = \mathrm{true}.$$

Если нет неоднозначности, мы будем опускать название игры и просто писать $\mathrm{win}_A(a)$.

Другими словами, a является выигрышной, если функция выигрыша равна true на всех векторах длины n, которые "расширяют" a. Это привело нас к введению следующего определения:

► Определение 4 (w*, W*). Для любого $a \in 2^k$, пусть ω_a будет множеством векторов в 2^n, которые расширяют a:

$$\omega_a := \{v \in 2^n \mid v_1 = a_1 \wedge \cdots \wedge v_k = a_k\} \in \Omega$$

и пусть W_a будет множеством всех булевых функций, которые истинны на ω_a:

$$W_a := \{\omega \in \Omega \mid \omega_a \Rightarrow_0 \omega\} \in \mathcal{S}.$$

Эти определения непосредственно влекут следующую лемму:

► Лемма 5 (winA_eq). Для любой булевой функции $F : 2^n \to 2$ и любой стратегии $a \in 2^k$ игрока A в соответствующей булевой игре, мы имеем:

$$\mathrm{win}_A(a) \iff F \in W_a.$$

Лемма 5 означает, что вероятность существования выигрышной стратегии удовлетворяет:

$$\mathbb{P}(\exists a : 2^k.\, \mathrm{win}_A(a)) = \mathbb{P}\left(\bigcup_{a \in 2^k} W_a\right). \tag{1}$$

Далее мы будем опираться на формулу включения-исключения, которую мы доказали в полной общности следующим образом:

► Теорема 6 (Pr*bigcup_incl_excl). Для любого конечного вероятностного пространства* $(\Omega, \mathcal{S}, \mathbb{P})$ *и любой последовательности событий $(S_i)*{0\leq i<n}$, мы имеем:

$$\mathbb{P}\left(\bigcup_{0 \le i < n} S_i\right) = \sum_{m=1}^{n} (-1)^{m-1} \sum_{\substack{J \subseteq \mathbb{N}[0,n) \\ \mathrm{Card}\, J = m}} \mathbb{P}\left(\bigcap_{j \in J} S_j\right). \tag{2}$$

Доказательство. Для доказательства этой теоремы в Coq мы формализуем небольшую теорию индикаторных функций $\mathrm{Ind}_S : \Omega \to \{0, 1\}$ для любого конечного множества $S \subseteq \Omega$, включая тот факт, что математическое ожидание удовлетворяет $\mathbb{E}(\mathrm{Ind}_S) = \mathbb{P}(S)$, затем формализуем алгебраическое доказательство формулы включения-исключения. Эти доказательства существенно опираются на теорию bigop библиотеки MathComp, а также на тактику "under", которую мы разработали в Ltac для удобного "переписывания под лямбдами" (например, под символом $\sum$). Эти тактические средства будут подробно рассмотрены в Разделе 6. ◀

Отсюда следует следующий результат:

► Теорема 7 (Pr_ex_winA). Для любого конечного вероятностного пространства $(\Omega, \mathcal{S}, \mathbb{P})$, вероятность того, что существует некоторая стратегия $a = (a_1, \ldots, a_k)$ игрока A, которая является выигрышной, удовлетворяет:

$$\mathbb{P}(\exists a : 2^k.\, \mathrm{win}_A(a)) = \sum_{a \in 2^k} \mathbb{P}(W_a) - \sum_{\substack{a, a' \in 2^k \\ a \neq a'}} \mathbb{P}(W_a \cap W_{a'}) + \cdots$$

$$= \sum_{m=1}^{2^k} (-1)^{m-1} \sum_{\substack{J \subset 2^k \\ \mathrm{Card}\, J = m}} \mathbb{P}\left(\bigcap_{a \in J} W_a\right).$$

Доказательство. Результат следует из (1) и (2) после переиндексации всех больших операторов $\bigcup$, $\sum$, $\bigcap$ натуральными числами вместо булевых векторов $a \in 2^k$, или наоборот. ◀

Теорема 7 применима с любой вероятностью $\mathbb{P}$, но с ней нелегко работать. В следующем разделе мы более подробно исследуем случай, когда $\mathbb{P}$ относительно проста.

Прежде чем уточнять Теорему 7 с конкретными определениями $\mathbb{P}$, мы формально изучим двойственный случай (т.е. существование выигрышной стратегии с точки зрения игрока B).

► Определение 8 (winB). Для любой игры $F : 2^k \times 2^{n-k} \to 2$, стратегия $b = (b_1, \ldots, b_{n-k})$ игрока B является выигрышной, если она выигрывает против любой стратегии $a \in 2^k$ игрока A:

$$\mathrm{win}_B[F](b) := \forall a \in 2^k.\, F(a, b) = \mathrm{false}.$$

Если нет неоднозначности, мы будем опускать название игры и просто писать $\mathrm{win}_B(b)$.

Первый результат состоит в том, чтобы показать, что игрок B выигрывает в данной игре тогда и только тогда, когда игрок A выигрывает в "двойственной игре".

► Лемма 9 (winB_eq). Любая булева игра $F : 2^k \times 2^{n-k} \to 2$ (с n переменными, k из которых контролируются игроком A) может быть ассоциирована с двойственной булевой игрой $F' : 2^{n-k} \times 2^k \to 2$ такой, что

$$\mathrm{win}_B[F](b) \iff \mathrm{win}_A[F'](b)$$

Доказательство. Сначала мы определяем двойственную игру $F' := \mathrm{bool\_game\_sym}(F)$, ассоциированную с F как:

$$F' := (b, a) \mapsto \neg F(a, b).$$

Затем мы определяем bool_game_sym' (обратную функцию к bool_game_sym) и показываем, что обе функции являются биекциями. В формальном описании соответствующие леммы названы bool_game_sym_bij и bool_game_sym'_bij. ◀

Отсюда мы выводим следующий результат, который связывает вероятность существования выигрышной стратегии для игрока B с соответствующей вероятностью для игрока A.

► Теорема 10 (Pr*ex_winB). Для любого конечного вероятностного пространства* $(\Omega, \mathcal{S}, \mathbb{P})$*, вероятность того, что существует некоторая стратегия $b = (b_1,\ldots,b$*{n-k})$ игрока B, которая является выигрышной, удовлетворяет:

$$\mathbb{P}(\exists b : 2^{n-k}.\, \mathrm{win}_B[F](b)) = \mathbb{P}(\exists a : 2^{n-k}.\, \mathrm{win}_A[F'](a)),$$

где $F' := \mathrm{bool\_game\_sym}(F)$.

Доказательство. Доказательство непосредственно следует из Леммы 9. ◀

Наконец, мы доказываем интуитивный факт, что события "$\exists a.\, \mathrm{win}_A(a)$" и "$\exists b.\, \mathrm{win}_B(b)$" не пересекаются, и следовательно их вероятности складываются:

► Лемма 11 (Pr_ex_winA_winB_disj). Для любого конечного вероятностного пространства $(\Omega, \mathcal{S}, \mathbb{P})$, мы имеем:

$$\mathbb{P}(\exists a.\, \mathrm{win}_A(a) \vee \exists b.\, \mathrm{win}_B(b)) = \mathbb{P}(\exists a.\, \mathrm{win}_A(a)) + \mathbb{P}(\exists b.\, \mathrm{win}_B(b)).$$

Доказательство. Учитывая определения win_A и win_B, для данной игры F и любых стратегий a и b, события "$\mathrm{win}_A(a)$" и "$\mathrm{win}_B(b)$" не пересекаются. Так что доказательство сводится к тому, чтобы поднять этот факт (рассматривая существование) и использовать аддитивность $\mathbb{P}$. ◀

Я сделаю перевод этого математического текста, сохраняя точность терминологии и форматирование.

3 Процесс Бернулли и выигрышные стратегии

В этом разделе мы по-прежнему рассматриваем пространство $\Omega = 2^{2^n}$ случайных булевых формул от n переменных, наделенное дискретной σ-алгеброй $\mathcal{S} = 2^{2^{2^n}}$, и связанные с ним булевы игры с параметром $0 \leq k \leq n$. Однако теперь мы предполагаем, что булевы формулы (в ДНФ) определяются случайным выбором булевых векторов, удовлетворяющих формулам.

Точнее, мы предполагаем, что вероятность принадлежности каждого вектора $v \in 2^n$ множеству истинности формулы F равна p, $(0 \leq p \leq 1)$. Как обычно, мы пишем $q = 1 - p$.

В дальнейшем мы будем часто отождествлять булевы функции $F : 2^n \to 2$ и их множества истинности $F^{-1}(\{\mathrm{true}\}) \in 2^{2^n}$. В формализации Coq различие между ними всегда делается явным, и функция, дающая множество истинности булевой функции, реализуется функцией

```
finset_of_bool_fun : ∀n : nat, bool_fun n -> {set bool_vec n}
```

и обратная к этой функции формализуется как функция DNF_of (дизъюнктивная нормальная форма).

Наша установка сводится к построению процесса Бернулли, то есть серии независимых испытаний Бернулли, чтобы определить, принадлежит ли каждый вектор $v \in 2^n$ множеству истинности F или нет. Мы получаем следующий результат:

► Лемма 12 (dist*BernoulliE).* Для любой $F \in \Omega$ вероятность элементарного события $\{F\}$ относительно рассматриваемой вероятности $\mathbb{P}_{n;p}$ (моделирующей серию из 2^n независимых испытаний Бернулли с параметром p) равна:_

$$\mathbb{P}_{n;p}(\{F\}) = p^m (1-p)^{2^n - m}$$

где m обозначает число векторов в множестве истинности F, а $2^n - m$ обозначает число векторов в множестве истинности отрицания F.

Доказательство. Доказательство (и его формальный аналог в Coq) непосредственно следует из определений. ◄

Теперь предположим, что выборы игрока A и B делаются одновременно. A выигрывает, если значение F истинно, в противном случае выигрывает B. Какова вероятность того, что A имеет выигрышную стратегию?

Сначала предположим, что стратегия a игрока A фиксирована, и вычислим вероятность того, что она является выигрышной. Сначала докажем следующее

► Лемма 13 (Pr*impliesO_Bern).* Пусть $S \subseteq 2^n$, и пусть $m := \mathrm{Card}\, S$. Тогда вероятность того, что F истинна на S удовлетворяет: $\mathbb{P}_{n;p}(S \Rightarrow_0 F) = p^m$._

Доказательство. Следуем следующему пути доказательства:

$$\begin{aligned}
\mathbb{P}_{n;p}(S \Rightarrow_0 F) &= \sum_{S \subseteq F} \mathbb{P}_{n;p}(\{F\}) \\
&= \sum_{S' \subseteq 2^n \setminus S} \mathbb{P}_{n;p}(\{F\}) \\
&\qquad F = S \cup S' \\
&= \sum_{S' \subseteq 2^n \setminus S} p^{\mathrm{Card}(S \cup S')} q^{2^n - \mathrm{Card}(S \cup S')} \text{ по Лемме 12} \\
&= \sum_{m'=0}^{2^n - m} \binom{2^n - m}{m'} p^{m+m'} q^{2^n - m - m'} \\
&= p^m \sum_{m'=0}^{2^n - m} \binom{2^n - m}{m'} p^{m'} q^{(2^n - m) - m'} \\
&= p^m (p+q)^{2^n - m} \\
&= p^m. \qquad \blacktriangleleft
\end{aligned}$$

► Лемма 14 (card*w_a_Bern).* Для любой стратегии a игрока A имеем_

$$\mathrm{Card}\, w_a = 2^{n-k}.$$

Доказательство. Эта лемма легко следует из того факта, что w_a является образом пространства стратегий 2^{n-k} игрока B при инъективной функции. ◄

Отсюда следует теорема, которая дает вероятность того, что фиксированная стратегия A является выигрышной:

► Теорема 15 (Pr*winA_Bern).* Для любой стратегии a игрока A имеем_

$$\mathbb{P}_{n;p}(\mathrm{win}_A(a)) = p^{2^{n-k}}.$$

Доказательство. Этот результат является непосредственным следствием Лемм 13 и 14. ◄

Теперь определим, какова вероятность того, что A имеет хотя бы одну выигрышную стратегию.
Сначала можно заметить следующее

► Лемма 16 (w*trivIset).* Множества истинности w_a (для $a \in J \subseteq 2^k$) попарно не пересекаются._

Доказательство. От противного: если бы у нас были $a, a' \in 2^k$ такие, что $w_a \neq w_{a'}$ и $w_a \cap w_{a'} \neq \emptyset$, то пусть $x \in w_a \cap w_{a'}$. Разворачивая Определение 4, это означает, что первые k битов x совпадают со всеми битами a, и аналогично для a'. Это означает, что $a = a'$ и, следовательно, $w_a = w_{a'}$, что противоречит исходной гипотезе. ◄

Лемма 16 подразумевает, что

$$\mathrm{Card}\left(\bigcup_{a\in J} w_a\right) = \sum_{a\in J} \mathrm{Card}\, w_a = \mathrm{Card}\, J \cdot 2^{n-k}. \qquad (3)$$

Теперь мы можем доказать следующее

► Теорема 17 (Pr*ex_winA_Bern).* Для любых n и k, если $\mathbb{P}_{n;p}$ следует схеме Бернулли, которую мы ранее построили, вероятность того, что игрок A имеет выигрышную стратегию, равна:_

$$\mathbb{P}_{n;p}(\exists a.\, \mathrm{win}_A(a)) = 1 - \left(1 - p^{2^{n-k}}\right)^{2^k}.$$

Доказательство. Благодаря Теореме 7, мы можем записать:

$$\begin{aligned}
\mathbb{P}_{n;p}(\exists a : 2^k.\, \mathrm{win}_A(a)) &= \sum_{m=1}^{2^k} (-1)^{m-1} \sum_{\substack{J\subseteq 2^k \\ \mathrm{Card}\, J = m}} \mathbb{P}_{n;p}\left(\bigcap_{a\in J} W_a\right) \\
&= \sum_{m=1}^{2^k} (-1)^{m-1} \sum_{\substack{J\subseteq 2^k \\ \mathrm{Card}\, J = m}} \mathbb{P}_{n;p}\left(\bigcap_{a\in J} [w_a \Rightarrow_0 F]\right) \\
&= \sum_{m=1}^{2^k} (-1)^{m-1} \sum_{\substack{J\subseteq 2^k \\ \mathrm{Card}\, J = m}} \mathbb{P}_{n;p}\left[\left(\bigcup_{a\in J} w_a\right) \Rightarrow_0 F\right] \\
&= \sum_{m=1}^{2^k} (-1)^{m-1} \sum_{\substack{J\subseteq 2^k \\ \mathrm{Card}\, J = m}} p^{(\mathrm{Card}(\bigcup_{a\in J} w_a))} \text{ по Лемме 13} \\
&= \sum_{m=1}^{2^k} (-1)^{m-1} \sum_{\substack{J\subseteq 2^k \\ \mathrm{Card}\, J = m}} p^{m\cdot 2^{n-k}} \text{ используя (3) и Лемму 14} \\
&= \sum_{m=1}^{2^k} (-1)^{m-1} \binom{2^k}{m} p^{m\cdot 2^{n-k}} \\
&= 1 - \sum_{m=0}^{2^k} \binom{2^k}{m} (-p^{2^{n-k}})^m 1^{2^k - m} \\
&= 1 - \left(1 - p^{2^{n-k}}\right)^{2^k}. \qquad \blacktriangleleft
\end{aligned}$$

По двойственности можно вывести существование выигрышной стратегии для игрока B:

► Следствие 18 (Pr*ex_winB_Bern).* Для любых p, n, k, если $\mathbb{P}_{n;p}$ обозначает рассматриваемую схему Бернулли (с параметрами $0 \leq p \leq 1$ и $n \in \mathbb{N}$) и если k обозначает число переменных, контролируемых игроком A, тогда вероятность того, что игрок B имеет выигрышную стратегию, равна:_

$$\mathbb{P}_{n;p}(\exists b : 2^{n-k}.\, \mathrm{win}_B(b)) = 1 - \left(1 - (1-p)^{2^k}\right)^{2^{n-k}}.$$

Доказательство. Результат следует из Теорем 10 и 17. Также, доказательство использует нашу тактику переписывания под лямбдами (она будет представлена в Разделе 6). ◄

Таблица 1

Вероятность того, что выигрышная стратегия не существует ни для A, ни для B ($n = 10$).

p\k	1	2	3	4	5	6	7	8	9
0.25	1.52e-184	5.11e-43	1.37e-6	0.525	0.997	1	0.998	0.367	4.46e-15
0.5	1.07e-64	6.68e-8	0.606	0.999	1	0.999	0.606	6.68e-8	1.07e-64
0.75	4.46e-15	0.367	0.998	1	0.997	0.525	1.37e-6	5.11e-43	1.52e-184

Таблица 2

Вероятность того, что выигрышная стратегия не существует ни для A, ни для B ($n = 20$).

p\k	1	2	3	4	5	6-10
0.25	1.27e-188231	2.04e-43307	2.15e-6005	1.99e-287	3.72e-2	1
0.5	1.32e-65504	2.74e-7348	1.61e-223	0.368	1	1
0.75	7.53e-14696	2.58e-446	0.135	1	1	1

p\k	11-15	16	17	18	19
0.25	1	1	0.135	2.58e-446	7.53e-14696
0.5	1	0.368	1.61e-223	2.74e-7348	1.32e-65504
0.75	1	1.99e-287	2.15e-6005	2.04e-43307	1.27e-188231

Примечание: В обеих таблицах значение 1 фактически означает число, чрезвычайно близкое к 1, но не точно 1.

► Следствие 19 (Pr*nex_winA_winB_Bern)*. Для любых p, n, k, если $\mathbb{P}_{n;p}$ обозначает рассматриваемую схему Бернулли (с параметрами $0 \leq p \leq 1$ и $n \in \mathbb{N}$) и если k обозначает число переменных, контролируемых игроком A, тогда вероятность того, что ни у одного игрока нет выигрышной стратегии, равна:_

$$\mathbb{P}_{n;p}\left(\neg\left((\exists a.\, \mathrm{win}_A(a)) \vee (\exists b.\, \mathrm{win}_B(b))\right)\right) = \left(1 - p^{2^{n-k}}\right)^{2^k} + \left(1 - (1-p)^{2^k}\right)^{2^{n-k}} - 1. \quad (4)$$

Доказательство. Результат следует из Леммы 11, Теоремы 17 и Следствия 18. ◄

3.1 Обсуждение

Приведенные выше вычисления могут показаться элементарными, но приводят к некоторым нетривиальным наблюдениям. Как мы можем видеть, существует значительная вероятность того, что выигрышной стратегии нет вообще. Например, если $p \in \{\frac{1}{4}, \frac{1}{2}, \frac{3}{4}\}$, $n \in \{10, 20\}$, $0 < k < n$, вероятность того, что выигрышная стратегия не существует ни для A, ни для B (см. Уравнение (4)) приведена в Таблицах 1 и 2 (значения были вычислены с помощью Sollya[5] с 3-значным десятичным выводом). В обеих таблицах следует отметить, что 1 фактически означает значение, чрезвычайно близкое к 1, но не точно 1.

Также можно заметить, что когда $p \in (0, 1)$ фиксировано, $k = c \cdot n$ для заданной константы $0 < c < 1$, и n стремится к $+\infty$, вероятность того, что выигрышная стратегия не существует ни для игрока A, ни для игрока B, стремится к 1.

Если (для некоторой игры F) выигрышная стратегия не существует ни для A, ни для B, тогда порядок ходов становится важным. Действительно, пусть a — произвольная стратегия A. Поскольку она не является выигрышной, существует хотя бы один b игрока B такой, что $F(a,b) = \mathrm{false}$. Если B делает свой выбор после A, он всегда может выиграть. Аналогично, если A делает свой выбор после B, он всегда может выиграть.

Мы подробнее рассмотрим это наблюдение и приведем мотивирующий пример в Приложении A.

Брэдфилд, Гутьеррес и Вулдридж отмечают [4] (как и некоторые другие авторы): "В том виде, как они обычно формулируются, булевы игры предполагают, что игроки делают свой выбор, не зная о выборе, сделанном другими игроками — это игры с одновременными ходами. Для многих ситуаций это явно нереалистично." Наш простой вероятностный анализ предоставляет прямой количественный аргумент в поддержку этого общего наблюдения.

---

[5] http://sollya.gforge.inria.fr/

4 Частичная информация о выборе оппонента

Теперь рассмотрим случай, когда A может иметь частичную информацию о выборах B перед тем, как сделать свой выбор. Без потери общности мы можем предположить, что он знает значения первых s переменных среди переменных $v_{k+1}, \ldots, v_n$, контролируемых B. Мы рассмотрим вероятность существования стратегий A таких, что для каждого вектора $b_{1:s} = (b_1, \ldots, b_s) \in 2^s$ существует стратегия $a \in 2^k$, которая выигрывает против любой стратегии $b \in 2^{n-k}$, где первые s значений совпадают с $b_{1:s}$.

Другими словами, мы заинтересованы в вероятности гарантированного выигрыша A, когда известны s выборов B среди $n-k$ (предполагая $0 \leq s \leq n-k$). Таким образом, мы вводим следующий предикат:

Определение 20 (winA_knowing)

Для любой игры $F : 2^k \times 2^{n-k} \to 2$ и любого $b_{1:s} \in 2^s$ мы говорим, что стратегия $a \in 2^k$ является выигрышной при знании $b_{1:s}$, если она выигрывает против всех профилей стратегий $(a,b) \in 2^k \times 2^{n-k}$, которые совместимы с $b_{1:s}$:

$$\mathrm{win}_A(a|b_{1:s}) := \forall b \in 2^{n-k}.\, \mathrm{compat\_knowing}(b_{1:s}, b) \implies F(a,b) = 1,$$

где

$$\mathrm{compat\_knowing}(b_{1:s}, b) := \forall i \in 2^s.\, (b_{1:s})_i = b_i.$$

Для связи этого предиката с предикатом из Определения 3, доказательство следующей леммы очевидно:

Лемма 21 (winA_knowingE)

Для любой игры $F : 2^k \times 2^{n-k} \to 2$ и любых бит-векторов $b_{1:s} \in 2^s$ и $a \in 2^k$ имеем:

$$\mathrm{win}_A[F](a|b_{1:s}) = \mathrm{win}_A[\mathrm{bgk}(F, b_{1:s})](a)$$

где $\mathrm{bgk}(F, b_{1:s}) : 2^k \times 2^{n-s-k}$ является булевой игрой, определенной как:

$$\mathrm{bgk}(F, b_{1:s})(a, b') = F(a, (b_{1:s}, b')).$$

Теперь, чтобы вычислить вероятность $\mathbb{P}_{n;p}(\forall b_{1:s} \in 2^s.\, \exists a \in 2^k.\, \mathrm{win}_A(a|b_{1:s}))$ в пространстве $(\Omega, \mathcal{S}, \mathbb{P}_{n;p})$, введенном в Разделе 3, мы сначала построим вероятностное пространство $(\Omega', \mathcal{S}', \mathbb{P}')$, которое является доказуемо изоморфным $(\Omega, \mathcal{S}, \mathbb{P}_{n;p})$, но проще в обращении.

Сначала отметим, что существует 2^s возможных булевых векторов $b_{1:s} = (b_1, \ldots, b_s)$, и для всех $b_{1:s}$ мы полагаем

$$B_{b_{1:s}} = \{v \in 2^n | v_{k+1} = b_1 \wedge \ldots \wedge v_{k+s} = b_s\}.$$

Семейство $(B_{b_{1:s}})_{b_{1:s} \in 2^s}$ образует разбиение 2^n (имеем $2^n = \bigcup_{b_{1:s} \in 2^s} B_{b_{1:s}}$, пересечения $B_{b_{1:s}}$ для различных $b_{1:s}$ пусты, и ни одно множество $B_{b_{1:s}}$ не пусто).

Затем мы определяем $\Omega_{b_{1:s}} := 2^{B_{b_{1:s}}}$ как множество всех подмножеств $B_{b_{1:s}}$ и показываем, что существует взаимно однозначное соответствие между $\Omega_{b_{1:s}}$ и $2^{2^{n-s}}$. Мы обозначим соответствующие биекции через $g : \Omega_{b_{1:s}} \to 2^{2^{n-s}}$ и $h : 2^{2^{n-s}} \to \Omega_{b_{1:s}}$. В формальной разработке соответствующие леммы названы bool_fun_of_OmegaB_bij и OmegaB_of_bool_fun_bij.

Далее мы рассматриваем вероятность $\mathbb{P}_{b_{1:s}} := \mathbb{P}_{n-s;p} \circ h^{-1}$, определенную как прямой образ (pushforward) распределения (относительно функции h) процесса Бернулли $\mathbb{P}_{n-s;p}$ с параметрами $n-s$ и p.

Затем мы рассматриваем произведение пространств $(\Omega', \mathcal{S}', \mathbb{P}')$, определенное как:

$$\begin{cases} \Omega' = \prod_{b_{1:s} \in 2^s} \Omega_{b_{1:s}} \\ \mathcal{S}' = 2^{\Omega'} \\ \mathbb{P}' = \bigotimes_{b_{1:s} \in 2^s} \mathbb{P}_{b_{1:s}} \end{cases}$$

Опираясь на функции g и h, мы наконец показываем, что существует взаимно однозначное соответствие между Ω' и $\Omega = 2^{2^n}$. Мы обозначим соответствующие биекции через $g' : \Omega' \to \Omega$ и $h' : \Omega \to \Omega'$. В формальной разработке соответствующие леммы названы bool_fun_of_Omega'_bij и Omega'_of_bool_fun_bij.

Теперь мы докажем, что пространства $(\Omega, \mathcal{S}, \mathbb{P}_{n;p})$ и $(\Omega', \mathcal{S}', \mathbb{P}')$ изоморфны:

Лемма 22 (isom_dist_Omega')

Вероятностное распределение $\mathbb{P}_{n;p}$ (определенное в Разделе 3 как процесс Бернулли с параметрами n и p) экстенсионально равно прямому образу распределения $\mathbb{P}'$ относительно функции g'.

Доказательство. В формальном доказательстве в Coq эта лемма сводится к разбиению выражения с большим оператором относительно разбиения 2^n, переиндексированию выражений с большими операторами полдюжины раз и переписыванию "лемм сокращения" для упрощения композиции биекции и ее обратной функции. Также использование нашей тактики under (см. Раздел 6) способствовало упрощению механизации этого доказательства. ◀

Ключевым ингредиентом для продолжения будет следующее

Лемма 23 (ProductDist.indep)

Дан конечный тип I и семейство конечных вероятностных пространств $(\Omega_i, \mathcal{S}_i = 2^{\Omega_i}, \mathbb{P}_i)_{i \in I}$, произведение пространств, определенное как

$$\begin{cases} \Omega_\Pi = \prod_{i \in I} \Omega_i \\ \mathcal{S}_\Pi = 2^{\Omega_\Pi} \\ \mathbb{P}_\Pi = \bigotimes_{i \in I} \mathbb{P}_i \end{cases}$$

таково, что проекции $(\pi_i : \Omega_\Pi \to \Omega_i)_{i \in I}$ являются независимыми случайными величинами. Другими словами, для любого семейства событий $(Q_i)_{i \in I} \in \prod_{i \in I} \mathcal{S}_i$ имеем:

$$\mathbb{P}_\Pi \left(\bigcap_{i \in I} \pi_i^{-1}(Q_i) \right) = \prod_{i \in I} \mathbb{P}_i(Q_i).$$

Теперь мы можем доказать следующее

Теорема 24 (Pr_ex_winA_knowing_Bern)

Для всех $p \in [0,1]$ и для всех целых чисел n, k, s, удовлетворяющих $0 \leq s \leq n-k \leq n$, если $\mathbb{P}_{n;p}$ является процессом Бернулли с параметрами n и p, определенным в Разделе 3, вероятность гарантированного выигрыша для игрока A, знающего s выборов игрока B среди его $n-k$ переменных, равна:

$$\mathbb{P}_{n;p}(\forall b_{1:s} \in 2^s. \, \exists a \in 2^k. \, \mathrm{win}_A(a | b_{1:s})) = \left(1 - \left(1 - p^{2^{n-k-s}}\right)^{2^k}\right)^{2^s}. \tag{5}$$

Доказательство. Мы следуем следующему пути доказательства:

$$\mathbb{P}_{n;p}(\forall b_{1:s} \in 2^s. \, \exists a \in 2^k. \, \mathrm{win}_A(a | b_{1:s}))$$

$$= \mathbb{P}_{n;p}\{F \in \Omega | \forall b_{1:s} \in 2^s. \exists a \in 2^k. \operatorname{win}_A[F](a|b_{1:s})\}$$

следовательно, используя Лемму 21

$$= \mathbb{P}_{n;p}\{F \in \Omega | \forall b_{1:s} \in 2^s. \exists a \in 2^k. \operatorname{win}_A[\operatorname{bgk}(F, b_{1:s})](a)\}$$

следовательно, используя Лемму 22

$$= (\mathbb{P}' \circ g'^{-1})\{F \in \Omega | \forall b_{1:s} \in 2^s. \exists a \in 2^k. \operatorname{win}_A[\operatorname{bgk}(F, b_{1:s})](a)\}$$

следовательно, используя элементарные факты о g, g' и функции bgk, определенной в Лемме 21

$$= \mathbb{P}'\{f \in \Omega' | \forall b_{1:s} \in 2^s. f(b_{1:s}) \in \{S \in \Omega_{b_{1:s}} | \exists a \in 2^k. \operatorname{win}_A[g(S)](a)\}\}$$

следовательно, используя Лемму 23

$$= \prod_{b_{1:s} \in 2^s} \mathbb{P}_{b_{1:s}}\{S \in \Omega_{b_{1:s}} | \exists a \in 2^k. \operatorname{win}_A[g(S)](a)\}$$

следовательно, по определению $\mathbb{P}_{b_{1:s}}$

$$= \prod_{b_{1:s} \in 2^s} (\mathbb{P}_{n-s;p} \circ h^{-1})\{S \in \Omega_{b_{1:s}} | \exists a \in 2^k. \operatorname{win}_A[g(S)](a)\}$$

следовательно, по определению g и h

$$= \prod_{b_{1:s} \in 2^s} \mathbb{P}_{n-s;p}\{F \in 2^{2^{n-s}} | \exists a \in 2^k. \operatorname{win}_A[F](a)\}$$

следовательно, используя Теорему 17 в случае случайных булевых функций с $n - s$ переменными

$$= \prod_{b_{1:s} \in 2^s} \left(1 - \left(1 - p^{2^{n-s-k}}\right)^{2^k}\right)$$

$$= \left(1 - \left(1 - p^{2^{n-k-s}}\right)^{2^k}\right)^{2^s}. \qquad (\blacktriangleleft)$$

Мы можем сравнить эту вероятность с вероятностью существования безусловно выигрышной стратегии, изученной в Разделе 3 (Теорема 17). Следующий раздел будет посвящен этому вопросу.

Замечание

В Теоремах 17 и 24 мы формально изучили вероятность гарантированного выигрыша (при знании частичной информации об оппоненте), то есть вероятность того, что для каждого значения, принимаемого первыми s переменными B[6], существует стратегия для A, которая выигрывает против всех стратегий B при этом фиксированном значении первых s переменных B. Эта проблема является чисто комбинаторной и не зависит от "предпочтений" B (относительно переменных, которые он контролирует). Поэтому эта вероятность обычно будет отличаться от вероятности негарантированного выигрыша для игрока A, так как на последнюю вероятность могут влиять предпочтения B для некоторых выборов, зависимость этих выборов от F и так далее.

---

[6] Теорема 17 является частным случаем Теоремы 24 ($s = 0$).

5 Вероятность гарантированной победы: скорость роста

Используя результат, полученный в Теореме 24, мы хотели бы изучить, как вероятность гарантированной победы растет с каждым битом информации о выборе B.

Для фиксированных значений $p \in (0, 1)$, $n, k \in \mathbb{N}$ таких, что $0 < k < n$, и для $0 \leq s \leq n - k$, обозначим через $g(s)$ величину, заданную в Уравнении (5).

Сначала отметим, что когда s стремится к $n - k$, вероятность гарантированной победы для A стремится к:

$$g(n-k) = \left(1 - \left(1 - p^{2^k}\right)^{2^{n-k}}\right)^{2^s} = \left(1 - (1-p)^{2^k}\right)^{2^{n-k}} = 1 - \underbrace{\left[1 - \left(1 - (1-p)^{2^k}\right)^{2^{n-k}}\right]}_{\text{вер. гарантированной победы для } B}$$

Тогда интересным вопросом может быть: каков порядок роста разности

$$\phi(s) := g(s) - g(0) \quad (\in [0,1])$$

относительно s? Следующий результат дает первый ответ на этот вопрос:

► **Теорема 25** (phi_ineq). *Для любых $p \in (0,1)$, $n,k \in \mathbb{N}$ таких, что $0 \le s \le n-k$, если выполняется следующее условие:**

$$2^k p^{2^{n-k-s}} < 1, \tag{6}$$

тогда имеем

$$\phi(s) > \left(2^{(k-1)2^s} - 2^k\right) p^{2^{n-k}}, \tag{7}$$

где

$$\phi(s) = g(s) - g(0) = \left(1 - \left(1 - p^{2^{n-k-s}}\right)^{2^k}\right)^{2^s} - \left(1 - \left(1 - p^{2^{n-k}}\right)^{2^k}\right).$$

В частности, условие (6) выполняется, как только выполняется следующее, более сильное условие:

$$s \le (n-k) - \log_2(k+1) + \log_2(|\log_2 p|). \tag{8}$$

Доказательство. Пусть $t = p^{2^{n-k-s}}$. По биномиальной формуле имеем:

$$1 - (1-t)^{2^k} = 2^k t - (2^k t)^2 \sum_{i=2}^{2^k} (-1)^i 2^{-2k} \binom{2^k}{i} t^{i-2}. \tag{9}$$

Заметим, что если выполняется (6), то есть если $2^k t < 1$, то абсолютное значение $(i+1)$-го члена суммы $\sum$ в (9) меньше, чем у i-го члена, поскольку он получается умножением на $((2^k - i)/(i+1))t < 2^k t$. Итак, если выполняется (6), то сумма (положительная) меньше или равна своему первому члену. Более того, первый член суммы $\sum$ в (9) равен $2^{-2k}\frac{2^k(2^k-1)}{2} < \frac{1}{2}$. Следовательно, если (6) выполняется для некоторых n, k, s, то из (9) получаем

$$1 - (1-t)^{2^k} \ge 2^k t - \frac{1}{2}(2^k t)^2 = 2^k t \left(1 - \frac{1}{2} 2^k t\right) > 2^{k-1} t. \tag{10}$$

Таким образом, при этих условиях

$$g(s) = \left(1 - \left(1 - p^{2^{n-k-s}}\right)^{2^k}\right)^{2^s} > 2^{(k-1)2^s} p^{2^{n-k}}. \tag{11}$$

Далее, аналогичный анализ, применённый к $\left(1 - \left(1 - p^{2^{n-k}}\right)^{2^k}\right)$ даёт оценку

$$g(0) = \left(1 - \left(1 - p^{2^{n-k}}\right)^{2^k}\right) = 2^k p^{2^{n-k}} - \sum_{i=1}^{2^k} \binom{2^k}{i} \left(-p^{2^{n-k}}\right)^i \le 2^k p^{2^{n-k}} \tag{12}$$

Объединяя (11) и (12), получаем следующее неравенство:

$$g(s) - g(0) > 2^{(k-1)2^s} p^{2^{n-k}} - 2^k p^{2^{n-k}} = \left(2^{(k-1)2^s} - 2^k\right) p^{2^{n-k}}. \tag{13}$$

Наконец, следующее условие очевидно сильнее, чем (6):

$$2^k p^{2^{n-k-s}} \le \frac{1}{2},$$

что эквивалентно

$$2^{n-k-s} \log_2 p \le -(k+1).$$

Поскольку $0 < p < 1$, мы можем записать вместо этого

$$2^{n-k-s}|\log_2 p| \geq (k+1).$$

Применяя логарифм второй раз, получаем

$$s \leq (n-k) - \log_2(k+1) + \log_2(|\log_2 p|),$$

что тем самым является достаточным условием для (6).

Например, если $p = \frac{1}{2}$, условие (8) становится

$$s \leq (n-k) - \log_2(k+1). \tag{14}$$

И если $0 < p < \frac{1}{2}$, то $\log_2(|\log_2 p|) > 0$, поэтому имеем $-\log_2(k+1) < -\log_2(k+1) + \log_2(|\log_2 p|)$, и, следовательно, мы также можем полагаться на условие (14).

Можно отметить, что неравенство (7) по существу дает порядок роста $2^{(k-1)2^s}$ относительно количества информации s (числа дополнительных битов, известных игроку A), что намного быстрее, чем обычные порядки роста s или 2^s.

Тем не менее, более детальное изучение поведения функции, описывающей рост $g(s)$ (вероятности гарантированной победы в зависимости от s), требует гораздо больше усилий и места, чем мы могли бы уделить в этой поисковой работе. Например, интуитивно ясно, что график этой функции имеет типичную форму "S-кривой" (см. Рисунок 1), но нелегко определить, где расположены критические точки; и для малых значений параметра s неравенство, которое мы получаем в (7), может быть слишком грубым для достаточно точного определения. Однако поведение этой функции g может представлять интерес для стратегического планирования обоих игроков. Это остается предметом будущих исследований.

6 Замечания о формальной структуре в системе доказательств Coq

6.1 Связанные работы по формальным библиотекам теории вероятностей

Было проведено несколько работ, посвященных формализации теории меры или теории вероятностей с использованием интерактивных систем доказательств. Некоторые из этих работ рассматривают только дискретную вероятность или сосредоточены на анализе рандомизированных алгоритмов; другие формализуют большие фрагменты теории меры вплоть до теории интегрирования Лебега.

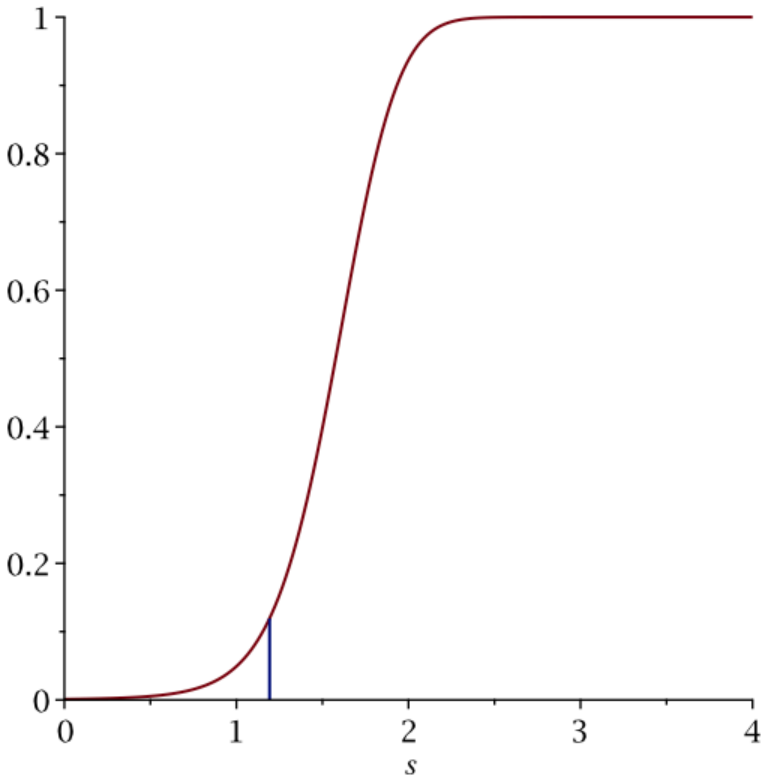


Рисунок 1 График функции $g(s)$ для параметров $p = \frac{1}{2}$, $n = 10$ и $k = 6$. Вертикальная линия при $s \approx 1.19$ указывает наибольшее $s \in \mathbb{R}$, удовлетворяющее (8).

Используя систему доказательств HOL, Hurd [13] разработал фреймворк для доказательства свойств рандомизированных программ, опираясь на формализацию теории меры и следуя подходу "монадической трансформации", который обеспечивает пользователя бесконечной последовательностью независимых, одинаково распределенных случайных величин $Bernoulli(\frac{1}{2})$.

Продолжая использовать систему доказательств HOL и основываясь на работе Hurd'a, Mhamdi, Hasan и Tahar [12, 15] разработали комплексную формализацию теории меры, включая теорию интегрирования Лебега.

Используя систему доказательств Coq, Audebaud и Paulin-Mohring [2] разработали библиотеку ALEA[7], которая предоставляет фреймворк для рассуждений о рандомизированных функциональных программах. В отличие от подхода Hurd'a, она не требует полной формализации теории меры: она построена на аксиоматизации интервала [0,1] в Coq и интерпретирует рандомизированные программы как (дискретные) распределения вероятностей.

Продолжая использовать формальную систему доказательств Coq, Affeldt, Hagiwara и Sénizergues [1] разработали библиотеку Infotheo[8], которая предоставляет формализацию теории информации. Эта библиотека содержит формализацию конечной теории вероятностей и существенно опирается на теории библиотеки MathComp[9].

Для разработки нашей библиотеки по случайным булевым играм мы решили опираться на библиотеку Infotheo. Хотя она работает только с конечными вероятностями, этой структуры было достаточно для формализации наших результатов и, более того, она позволила нам воспользоваться возможностями библиотеки SSReflect/MathComp. В оставшейся части этого раздела мы кратко изложим основные понятия, которые мы использовали из библиотеки MathComp, и представим наши связанные вклады (в разделе 6.2), затем опишем общую структуру теории вероятностей Infotheo и представим наши связанные вклады (в разделе 6.3).

[7] https://www.lri.fr/~paulin/ALEA/
[8] https://staff.aist.go.jp/reynald.affeldt/shannon
[9] https://math-comp.github.io/math-comp/

6.2 MathComp и наши связанные вклады

Библиотека MathComp возникла в рамках проекта Mathematical Components, целью которого была формализация Теоремы о нечетном порядке в системе доказательств Coq [9], с организацией формальных доказательств в компоненты для создания переиспользуемой библиотеки математических фактов. Она построена на SSReflect, расширении языка доказательств Coq, которое имеет встроенную поддержку так называемой малой рефлексии (и в частности булевой рефлексии) и часто приводит к лаконичным скриптам доказательств.

Для нашей библиотеки случайных булевых игр мы особенно использовали следующие библиотеки: *(i)* fintype для конечных типов с разрешимым равенством, *(ii)* finfun для функций над конечными доменами, *(iii)* finset для конечных множеств, *(iv)* bigop для свойств "больших операторов".

Большие операторы и переписывание под лямбдами

Что касается больших операторов, таких как $\sum$, $\prod$, $\cap$ или $\cup$, они формализованы в MathComp как функция высшего порядка bigop, которая принимает несколько аргументов, включая функцию, определяющую "предикат домена" и "общий терм". Например, сумма

$$\sum_{\substack{i=1 \\ i \text{ odd}}}^{4} i^2$$

может быть формально записана как \sum_(1 <= i < 5 | odd i) i^2, что сводится к следующему терму, если избавиться от нотации \sum:

```
bigop 0 (index_iota 1 5) (fun i:nat => BigBody i addn (odd i) (i^2))
```

Если мы хотим преобразовать такое выражение большого оператора путем переписывания его предиката домена или общего терма, могут быть использованы следующие две леммы MathComp для больших операторов.

```
eq_bigr :
  forall (R : Type) (idx : R) (op : R -> R -> R) (I : Type)
  (r : seq I) (P : pred I) (F1 F2 : I -> R),
  (forall i : I, P i -> F1 i = F2 i) ->
  \big[op/idx]_(i <- r | P i) F1 i = \big[op/idx]_(i <- r | P i) F2 i
```

```
eq_bigl :
  forall (R : Type) (idx : R) (op : R -> R -> R) (I : Type)
  (r : seq I) (P1 P2 : pred I) (F : I -> R),
  P1 =1 P2 ->
  \big[op/idx]_(i <- r | P1 i) F i = \big[op/idx]_(i <- r | P2 i) F i
```

Тем не менее, применение их напрямую потребовало бы предоставить весь терм, соответствующий функции, которую мы хотим получить.

Поэтому мы разработали тактику Coq "under" для переписывания под лямбдами больших операторов. Обобщенная версия нашей тактики, также применимая для понятий MathComp, таких как матрицы, многочлены и так далее, доступна онлайн по адресу https://github.com/erikmd/ssr-under-tac, и мы планируем представить ее для возможного включения в MathComp.

Ниже приведен типичный пример использования этой обобщенной реализации тактики under.

Для цели, которая выглядит как:

```
A : finType
n : nat
F : A -> nat
============================
0 <= \sum_(0 <= k < n)
```

```
      \sum_(J in {set A} | #|J| &: [set: A]| == k)
      \sum_(j in J) F j
```

скрипт доказательства

```
under eq_bigr [k Hk] under eq_bigl [J] rewrite setIT.
```

даст следующую цель:

```
A : finType
n : nat
F : A -> nat
============================
0 <= \sum_(0 <= k < n)
      \sum_(J in {set A} | #|J| == k)
      \sum_(j in J) F j
```

Зависимое произведение конечных типов

MathComp имеет встроенную поддержку конечных функций: для любых (A:finType) и (T:Type), нотация {ffun A -> T} обозначает тип конечных функций из A в T. Если n обозначает мощность A, эти функции представлены n-кортежем элементов T, что позволяет получить удобные свойства, такие как экстенсиональность конечных функций, которые в противном случае не выполнялись бы в конструктивной, интенсиональной логике Coq.

Если T также является конечным типом, то библиотека MathComp позволяет автоматически получить (благодаря выводу типов и так называемым каноническим структурам) структуру конечного типа для самого типа {ffun A -> T}. Таким образом, эта конструкция сводится к недепендентному произведению finType.

Однако для формализации наших результатов и в частности для построения типа Ω', который появляется в разделе 4, нам пришлось формализовать зависимое произведение конечного семейства конечных типов. Этот материал собран в файле fprod.v, который предоставляет тип fprod, некоторые нотации в стиле MathComp и несколько вспомогательных результатов, таких как леммы fprodP и fprodE, чья сигнатура выглядит следующим образом:

```
fprod : forall I : finType, (I -> finType) -> finType

fprodP : forall (I : finType) (T_ : I -> finType) (f1 f2: fprod I T_),
         (forall x : I, f1 x = f2 x) <-> f1 = f2

fprodE : forall (I : finType) (T_ : I -> finType)
                (g : forall i : I, T_ i) (x : I),
         [fprod i => g i] x = g x
```

Эта теория включает доказательства с зависимыми типами, и для облегчения процесса формализации мы старались следовать стилю формализации MathComp насколько это возможно, используя функции с конечными функциями, с булевыми условиями и так далее. Это позволило нам опираться на экстенсиональность функций, аксиому K Алтенкирха-Штрайхера и доказательную иррелевантность, которые могут использоваться "без аксиом" в разрешимом фрагменте конечных типов MathComp.

6.3 Infotheo и наши связанные вклады

Библиотека Infotheo опирается на MathComp, а также на теорию Reals из стандартной библиотеки Coq. Среди теорий Infotheo теория proba была отправной точкой нашей формализации. Она сначала определяет распределения как зависимую запись dist, собирающую функцию pmf, которая дает вероятность каждого элементарного события, и доказательство того, что сумма этих вероятностей равна 1:

```
Record dist (A : finType) :=
  mkDist { pmf :> A -> R+ ;
           pmf1 : \rsum_(a in A) pmf a = 1 }.
```

Затем она определяет вероятность подмножества A как сумму вероятностей всех элементарных событий в A:

```
Definition Pr (A : finType) (P : dist A) (E : {set A}) :=
\rsum_(a in E) P a.
```

Затем в этой структуре предоставляются базовые свойства вероятности и математического ожидания.

На основе теорий Infotheo мы разработали следующие вклады:
(i) формализация прямого распределения dist_img с соответствующей леммой

```
Lemma Pr_dist_img :
  forall {A B : finType} (X : A -> B) (PA : dist A) (E : {set B}),
  Pr (dist_img X PA) E = Pr PA (X @^-1: E).
```

(ii) формальное доказательство общей версии теоремы включения-исключения, которую мы представили выше в Теореме 6; *(iii)* произведение распределения семейства распределений, чья сигнатура выглядит следующим образом:

```
ProductDist.d :
  forall (I : finType) (T_ : I -> finType),
  (forall i : I, dist (T_ i)) -> dist (fprod I T_)
```

Связанный результат о независимости был представлен выше как Лемма 23.

Я переведу этот текст на русский язык, сохраняя форматирование Markdown и математические обозначения.

7 Заключение

В данной работе мы использовали основы теории булевых игр. В этом смысле наша работа, очевидно, связана с этой областью. Однако, насколько нам известно, идея применения теории вероятностей к определенному классу булевых игр в целом (в отличие от просто случайных стратегий) является новой. Анализ целого класса игр позволяет обнаружить некоторые количественные свойства этих игр, которые было бы трудно выявить при изучении отдельной игры.

Кроме того, мы использовали теорию типов и интерактивное доказательство теорем для формализации наших результатов, чтобы обеспечить надежные гарантии их корректности, а также расширить существующие формальные библиотеки новыми элементами.

В частности, мы доказали замкнутую формулу для вероятности существования выигрышных стратегий в этих случайных булевых играх. Мы специализировали этот результат для вероятностного распределения на булевых функциях, которые генерируются схемой Бернулли на булевых векторах с любой вероятностью p в качестве параметра (можно отметить, что эта постановка включает более простой случай, когда все булевы функции имеют одинаковую вероятность: этот последний случай соответствует выбору $p = \frac{1}{2}$ в нашей постановке).

В данной работе наши методы оставались элементарными, но они позволили оценить относительную важность случаев, когда игроки используют одновременные и альтернативные ходы. Другим интересным феноменом, на наш взгляд, является рост вероятности выигрыша как функции информации о выборе противника. По существу, он намного быстрее, чем обычные 2^s, где s — количество информации (число дополнительных битов), известное игроку. Этот феномен подчеркивает различие между информацией, необходимой для выигрыша, и "мерой знания" о противнике и его стратегиях.

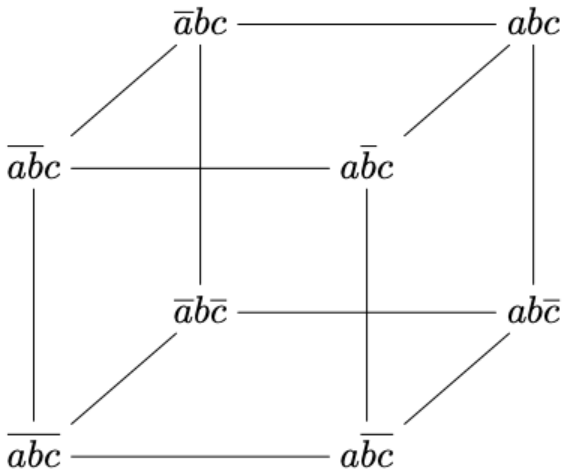
Мы уже упоминали важность машинной проверки верификации для игр между автономными программами (встроенные системы).

В качестве будущей работы мы планируем рассмотреть более общие классы вероятностных распределений и исследовать "вес" информации относительно выигрыша в этой более общей постановке.

Мы также планируем более подробно рассмотреть связь с алгоритмическими играми [6].

A Негарантированная победа: Когда порядок выбора имеет значение

Рассмотрим пример с тремя переменными a, b, c и двумя игроками: Алисой, которая контролирует a, и Бобом, который контролирует b, c. Рассмотрим все возможные булевы функции в качестве функций выигрыша. Существует 256 таких функций, которые могут быть идентифицированы с подмножествами узлов куба ниже. Каждое подмножество интерпретируется как дизъюнкция конъюнкций в узлах.



Имеет смысл проанализировать эту ситуацию чисто комбинаторным способом, прежде чем мы рассмотрим случайно сгенерированные функции выигрыша. Мы отмечаем следующие факты:

- У Алисы есть безусловно выигрышная стратегия в 31 случае (эти случаи соответствуют всем подмножествам, которые содержат все узлы либо грани с a, либо грани с $\bar{a}$; количество подмножеств легко подсчитывается по формуле включений-исключений).
- У Боба есть безусловно выигрышная стратегия в 175 случаях (случаи соответствуют подмножествам, которые не пересекаются с одним из четырех ребер, определяемых выбором двух литералов среди b, c, $\bar{b}$, $\bar{c}$; число подсчитывается как указано выше).
- Существует 50 случаев, когда ни у Алисы, ни у Боба нет безусловно выигрышной стратегии. В этих случаях порядок выбора имеет значение:
  - Если Алиса выбирает значение a первой, то у Боба есть выигрышная стратегия (он может выиграть во всех этих случаях).
  - Аналогично, если Боб выбирает значения b, c первым, то Алиса может выиграть во всех этих случаях.

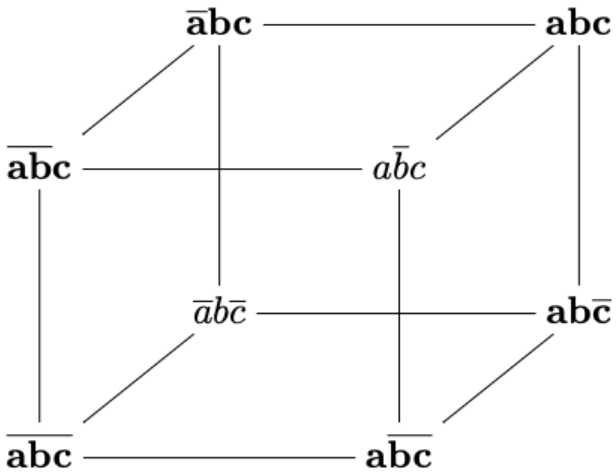
Теперь рассмотрим более подробно случай, когда порядок выборов $B - A - B$. Фактически, здесь нам нужно различать три подслучая:

1. Боб может дать значение любой из b, c на своем первом шаге.
2. На своем первом шаге Боб дает значение b, а на втором c.
3. На своем первом шаге Боб дает значение c, а на втором b.

Можно отметить, что эти три варианта могут соответствовать предпочтениям или обязательствам (дополнительным ограничениям) относительно Боба, в соответствии с замечанием в конце Раздела 4 (страница 12). Рассмотрим эти три подслучая подробнее.

1. Выбор Боба может интерпретироваться как выбор одной из четырех граней куба, соответствующих b, $\bar{b}$, c, $\bar{c}$ соответственно. Существует четыре случая, когда Алиса может выиграть, если она знает первый выбор Боба. Одно

подмножество показано ниже жирным шрифтом, остальные получаются вращением. (Мы исключаем случаи безусловного выигрыша, которые были подсчитаны ранее.)



В показанном выше случае, если Боб выбрал $b = \text{true}$, тогда Алиса должна выбрать $a = \text{true}$ и выигрывает, потому что оставшаяся формула будет $c \vee \bar{c}$.

2. Если на первом шаге Боб должен выбрать значение b, то это можно рассматривать как выбор одной из двух граней куба, соответствующих b или $\bar{b}$. Это дает Алисе больше возможностей для победы. Действительно, она может выиграть, если подмножество узлов включает либо $\overline{abc}$, $\overline{abc}$, $ab\bar{c}$, abc, либо $\overline{abc}$, abc, $a\bar{b}\bar{c}$, $\overline{abc}$. Мы можем добавить один или несколько узлов к каждому подмножеству из четырех, но если мы исключим ранее рассмотренные случаи, у нас будет еще 12 случаев, когда Алиса может выиграть.
3. Аналогичный анализ показывает, что будет 12 случаев (не рассмотренных ранее), где Алиса может выиграть, если Боб должен выбрать значение c первым.

Важно заметить, что выборы Алисы и Боба не обязательно интерпретируются как выборы логических значений a, b, c. Эта модель может использоваться для моделирования любого бинарного выбора. Действительно, пусть $a = \text{true}$ означает выбор некоторого значения v_a, а $a = \text{false}$ означает выбор v'_a Алисой. Аналогично, Боб может выбрать одно из v_b, v'_b и одно из v_c, v'_c. Вместо конъюнкции литералов (например, $\overline{abc}$) возьмем для каждой такой конъюнкции предикат[10] $P_{\overline{abc}}(x, y, z)$, который истинен тогда и только тогда, когда $x = v_a$, $y = v'_b$, $z = v'_c$. Вместо рассмотрения дизъюнкции этих конъюнкций, возьмем дизъюнкцию соответствующих предикатов. Оказывается, что логическое значение результата будет в точности логическим значением функции выигрыша, представленной ДНФ (или булевой функцией).

[10]определено для $(x, y, z) \in \{v_a, v'_a\} \times \{v_b, v'_b\} \times \{v_c, v'_c\}$

Та же идея может быть использована для моделирования рынков (выбор $a = \text{true}$ может означать, что Алиса заказывает покупку определенного продукта a, а $a = \text{false}$ — что она заказывает продажу, и наличие abc означает, что она получает прибыль, когда покупает в тот же момент, когда Боб продает два своих продукта).

Этот анализ также ясно показывает, какова может быть роль введения случайного выбора функций выплат. Это учитывает определенную степень непредсказуемости в реальной ситуации. Обратите внимание, что это не устраняет некоторую «геометрическую структуру», представленную в приведенном выше примере.

Однако, как мы подчеркивали ранее, мы намерены использовать вероятностный подход в основном для анализа совокупности игр со всеми возможными булевыми функциями в качестве функции выплат, а не для рассмотрения одной игры со случайно выбранной функцией выплат (хотя в некоторых случаях это может иметь смысл).

Выбор вероятностного распределения повлияет на относительный «вес» случаев, которые мы рассмотрели выше в чисто комбинаторном смысле, и должен быть принят во внимание при добавлении дополнительных условий, таких как порядок ходов или доступ к информации.

Например, если параметр вероятности p принимает значение $\frac{1}{2}$ (то есть если мы сосредоточимся на примере $\mathbb{P}_{3;\frac{1}{2}}$ процесса Бернулли, представленного в Разделе 3), это даст равномерное распределение на 256 случаях, рассмотренных в приложении.