Vers une preuve formelle du théorème de Pick en Coq

Farzad Sehat, Nicolas Magaud et Julien Narboux

Université de Strasbourg

Réunion Galapagos, 17-18 décembre 2008, Strasbourg, France

Plan

Motivations

Pourquoi le théorème de Pick ?

- Conférence de Mathématiques (Juillet 1999)
  Paul et Jack Abad : "The Hundred Greatest Theorems"

Motivations

Pourquoi le théorème de Pick ?

- Conférence de Mathématiques (Juillet 1999)
  Paul et Jack Abad : "The Hundred Greatest Theorems"
  - 1er - L'irrationalité de la racine carré de 2

Motivations

Pourquoi le théorème de Pick ?

- Conférence de Mathématiques (Juillet 1999)
  Paul et Jack Abad : "The Hundred Greatest Theorems"
  - 1er - L'irrationalité de la racine carré de 2
  - ...

Motivations

Pourquoi le théorème de Pick ?

- Conférence de Mathématiques (Juillet 1999)
  Paul et Jack Abad : "The Hundred Greatest Theorems"
  - 1er - L'irrationalité de la racine carré de 2
  - ...
  - 92ème - Théorème de Pick

Motivations

Pourquoi le théorème de Pick ?

- Conférence de Mathématiques (Juillet 1999)
  Paul et Jack Abad : "The Hundred Greatest Theorems"
  - 1er - L'irrationalité de la racine carré de 2
  - ...
  - 92ème - Théorème de Pick
- la liste a été reprise par Freek Wiedijk de l'Université de Radboud

Motivations

Pourquoi le théorème de Pick ?

- Conférence de Mathématiques (Juillet 1999)
  Paul et Jack Abad : "The Hundred Greatest Theorems"
  - 1er - L'irrationalité de la racine carré de 2
  - ...
  - 92ème - Théorème de Pick
- la liste a été reprise par Freek Wiedijk de l'Université de Radboud
  - 81% ont été formalisés

Pourquoi le théorème de Pick ?

- Conférence de Mathématiques (Juillet 1999)
  Paul et Jack Abad : "The Hundred Greatest Theorems"
  - 1er - L'irrationalité de la racine carré de 2
  - ...
  - 92ème - Théorème de Pick
- la liste a été reprise par Freek Wiedijk de l'Université de Radboud
  - 81% ont été formalisés
  -

HOL Light	70
Mizar	45
ProofPower	42
Isabelle	40
Coq	40
PVS	15
nqthm/ACL2	12
NuPRL/MetaPRL	8

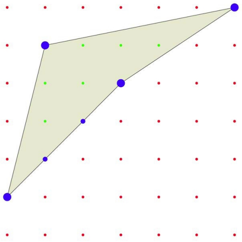
Le théorème de Pick

Théorème (George Alexander Pick 1899)

Soit un polygone simple construit à partir de point de $\mathbb{Z}^2$, soit A l'aire de ce polygone, soit i le nombre de points intérieurs au polygone ; soit b le nombre de points du bord du polygone alors :

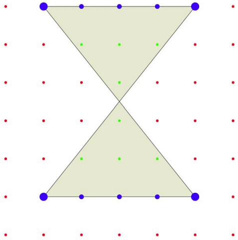
$$A = i + \frac{1}{2}b - 1$$

Exemple : polygone simple



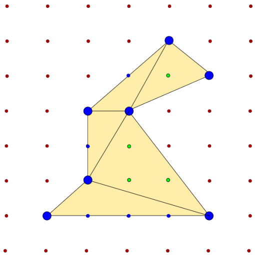
Dans l'exemple donné par la figure ci-dessus, nous avons $i = 6$ et $b = 6$, ainsi, l'aire est $A = 6 + \frac{6}{2} - 1 = 8$ (unités carrées).

Contre-exemple : polygone croisé



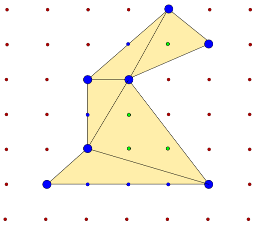
Attention, pour que le théorème soit vrai, il est nécessaire que le polygone soit simple comme le montre le contre exemple ci-dessus.

Preuve informelle



1. Triangulation

Preuve informelle



1. Triangulation
2. Induction sur le nombre de triangles composant la triangulation

Cas d'induction

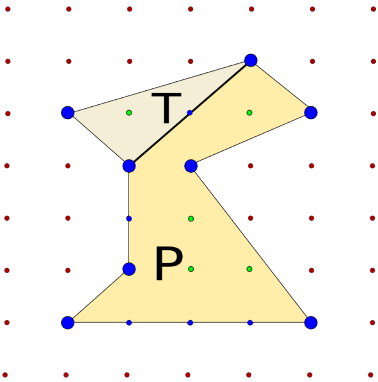
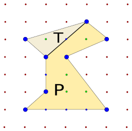


FIG.: Décomposition du polygone Q en un polygone P et triangle T .

Cas d'induction

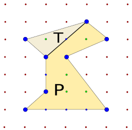


Etant donné un polygone Q construit en accolant à un côté d'un polygone P un triangle T.

$$A_Q = A_P + A_T$$

Cas d'induction

Etant donné un polygone Q construit en accolant à un côté d'un polygone P un triangle T.



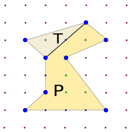
$$A_Q = A_P + A_T$$

Comme le théorème de Pick est supposé vrai pour P et T on a :

$$A_Q = i_P + \frac{1}{2}b_P - 1 \ + \ i_T + \frac{1}{2}b_T - 1$$

Cas d'induction

Etant donné un polygone Q construit en accolant à un côté d'un polygone P un triangle T.



$$A_Q = A_P + A_T$$

Comme le théorème de Pick est supposé vrai pour P et T on a :

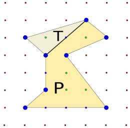
$$A_Q = i_P + \frac{1}{2} b_P - 1 \; + \; i_T + \frac{1}{2} b_T - 1$$

Soit c le nombre de points sur le côté commun à P et T. On a :

$$i_Q = (i_P + i_T) + (c - 2)$$

$$b_Q = (b_P - c) + (b_T - c) + 2$$

Cas d'induction



Etant donné un polygone Q construit en accolant à un côté d'un polygone P un triangle T.

$$A_Q = A_P + A_T$$

Comme le théorème de Pick est supposé vrai pour P et T on a :

$$A_Q = i_P + \frac{1}{2}b_P - 1 \;+\; i_T + \frac{1}{2}b_T - 1$$

Soit c le nombre de points sur le côté commun à P et T. On a :

$$i_Q = (i_P + i_T) + (c-2)$$

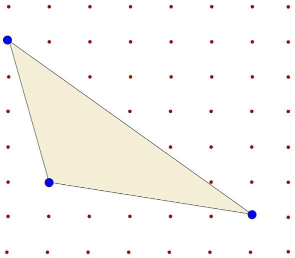
$$b_Q = (b_P - c) + (b_T - c) + 2$$

On en déduit que :

$$A_Q = i_Q - (c-2) + \frac{1}{2}(b_Q + 2(c-2) + 2) - 2$$

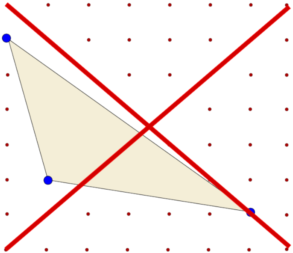
$$A_Q = i_Q + \frac{1}{2}b_Q - 1$$

Cas de base



Le triangle quelconque. . .

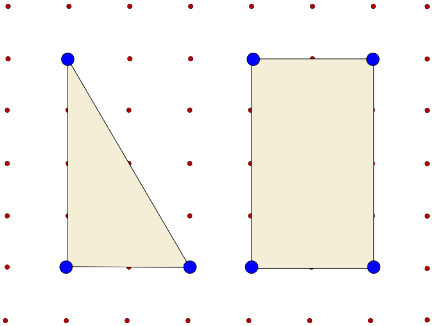
Cas de base



. . .est une figure trop complexe !

Cas de base

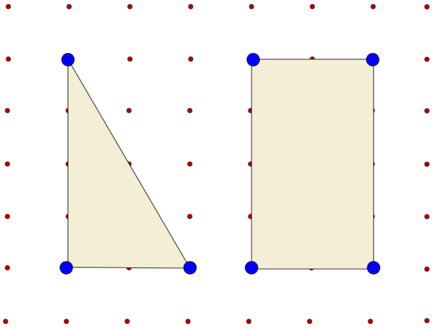
On se ramène à des figures plus simples :



- Côtés parallèles aux axes

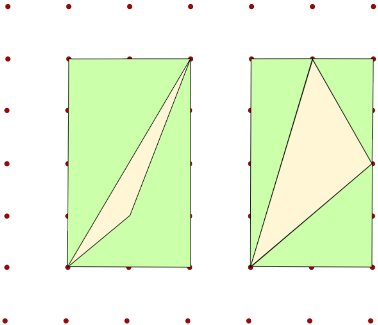
Cas de base

On se ramène à des figures plus simples :



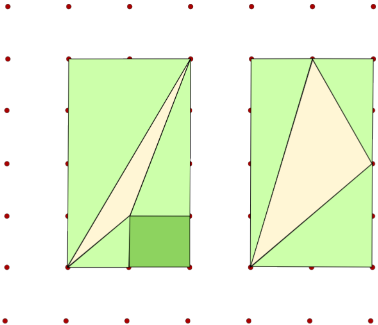
- Côtés parallèles aux axes
- Calcul du nombre de points à l'intérieur et sur le bord facilité

Cas de base



- Rectangle englobant

Cas de base



- Rectangle englobant
- Deux cas de décomposition possible

Preuve formelle

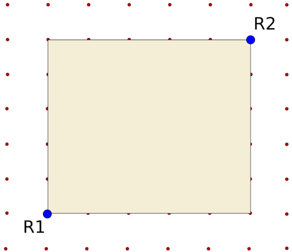
Structures utilisées pour les entités géométriques (Points, Rectangle, Triangle, etc) :

```
Record Point : Set :=
    cPoint { X : Z; Y : Z }.

Record Triangle : Set :=
    cTriangle { T1 : Point; T2 : Point; T3 : Point }.
```

Définitions

Le rectangle est défini par deux sommets opposés :




```
Record Rectangle : Set :=
    cRectangle { R1 : Point; R2 : Point }.
```

Définitions

Le nombre de points sur un segment :

```
Definition nb_pts (P1 P2 : Point) : Z :=
    let dX : Z := (X P2) - (X P1) in
    let dY : Z := (Y P2) - (Y P1) in
        (Zgcd dX dY).
```

Définitions

Le nombre de points sur un segment :

```
Definition nb_pts (P1 P2 : Point) : Z :=
    let dX : Z := (X P2) - (X P1) in
    let dY : Z := (Y P2) - (Y P1) in
        (Zgcd dX dY).
```

- Preuve en cours ...

Définitions

Le nombre de points sur un segment :

```
Definition nb_pts (P1 P2 : Point) : Z :=
    let dX : Z := (X P2) - (X P1) in
    let dY : Z := (Y P2) - (Y P1) in
        (Zgcd dX dY).
```

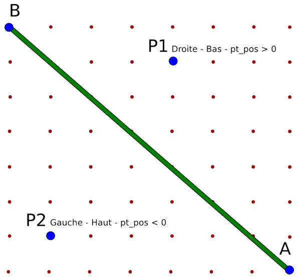
- Preuve en cours ...
- Pour se convaincre que cette définition est raisonnable :

```
Lemma nb_pts_v_seg :
    forall P1 P2 : Point,
    X P1 = X P2 ->
        nb_pts P1 P2 = Zabs (Y P2 - Y P1).

Lemma nb_pts_sym :
    forall P1 P2 : Point,
        nb_pts P1 P2 = nb_pts P2 P1.
```

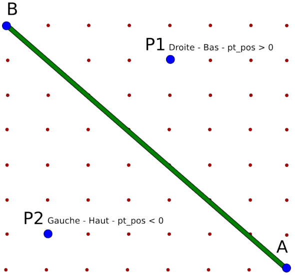
Définitions

La position d'un point par rapport à un segment :



Définitions

La position d'un point par rapport à un segment :

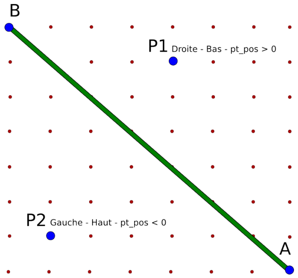


Difficulté :

- Le théorème de Pick est faux pour les triangles applatis

Définitions

La position d'un point par rapport à un segment :



Difficulté :

- Le théorème de Pick est faux pour les triangles applatis
- Hypothèse :

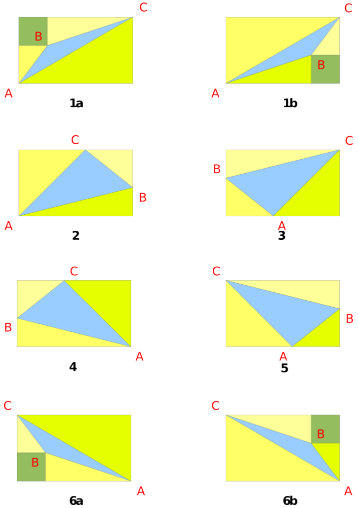
$$\textit{soit un triangle } A\ B\ C,\ \textit{pt\_pos}\ B\ A\ C\ \neq\ 0$$

Cas de base

- Triangles triés selon les ordonnées des points qui le compose

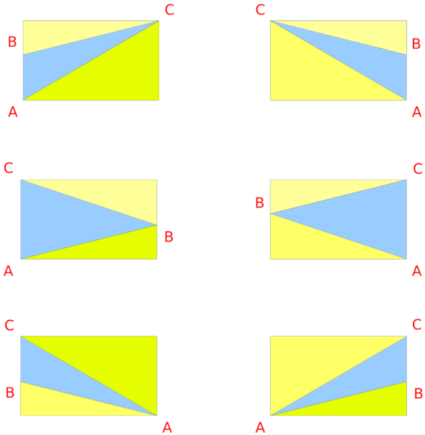
Cas de base

- Triangles triés selon les ordonnées des points qui le compose
- 6 conformations de base générés selon les ordres des abscisses



Cas de base

- Ordres larges $\Rightarrow$ triangles dégénérés :



Cas de base

Lemme central de la preuve du cas de base :

```
Lemma sum_of_areas :
    forall A B C : Point ,
    let t := cTriangle A B C in
    let r := encp_rect t in
    let cp := rtrigs_mrect t in
    let lt := fst cp in
    let mr := snd cp in
    Y A <= Y B <= Y C -> pt_pos B A C <> 0 ->
    trig_area_t t =
        (rect_area_t r) -
        (fold_left Zplus (map rect_area_t mr) 0) -
        (fold_left Zplus (map trig_area_t lt) 0).
```

Techniques utilisées

Quelques astuces :

- Multiplication par 2 pour rester dans $\mathbb{Z}$:

```
Definition trig_pick_area (t : Triangle) :=
    trig_ip t + ((trig_bp t) / 2) - 1.

Definition trig_pick_area_t (t : Triangle) :=
    trig_ip_t t + trig_bp t - 2.
```

Techniques utilisées

- Triangles triés par leur ordonnés pour restreindre le nombre de cas à traiter

Techniques utilisées

- Triangles triés par leur ordonnés pour restreindre le nombre de cas à traiter
- Nombreuses tactiques :

Techniques utilisées

- Triangles triés par leur ordonnés pour restreindre le nombre de cas à traiter
- Nombreuses tactiques :
  - Simplification d'expressions

Techniques utilisées

- Triangles triés par leur ordonnés pour restreindre le nombre de cas à traiter
- Nombreuses tactiques :
  - Simplification d'expressions
  - Simplification de valeur absolues

Techniques utilisées

- Triangles triés par leur ordonnés pour restreindre le nombre de cas à traiter
- Nombreuses tactiques :
  - Simplification d'expressions
  - Simplification de valeur absolues
  - Simplification de PGCD

Techniques utilisées

- Triangles triés par leur ordonnés pour restreindre le nombre de cas à traiter
- Nombreuses tactiques :
  - Simplification d'expressions
  - Simplification de valeur absolues
  - Simplification de PGCD
  - ...

Cas d'induction

Hypothèse : on suppose qu'on a une bonne triangulation

```
Theorem Pick :
    forall tr: pre_triangulation,
    is_proper_triangulation tr ->
          area_t tr = 2 * nb_ip tr + nb_bp tr - 2.
```

Vue d'ensemble et conclusion

	Spécifications	Preuves	Commentaires	Total
Cas de base	920	1518	588	77%
Induction	34	56	6	3%
Général	455	329	0	20%
Total	1409	1903	594	3906

La force brute ne fonctionne pas, il est *nécessaire* de raisonner en utilisant les symétries.

Perspectives

- Finir les preuves :

Perspectives

- Finir les preuves :
  - existence de la triangulation des polygones simples

Perspectives

- Finir les preuves :
  - existence de la triangulation des polygones simples
  - nombre de points sur un segment

Perspectives

- Finir les preuves :
  - existence de la triangulation des polygones simples
  - nombre de points sur un segment
  - nombre de points à l'intérieur d'un triangle

Perspectives

- Finir les preuves :
  - existence de la triangulation des polygones simples
  - nombre de points sur un segment
  - nombre de points à l'intérieur d'un triangle
- ...

Perspectives

- Finir les preuves :
  - existence de la triangulation des polygones simples
  - nombre de points sur un segment
  - nombre de points à l'intérieur d'un triangle
- ...
- Applications en compilation (cf travaux de Philippe Clauss)

```
for i := 0 to n do
   for j := 0 to i do
       for k := 0 to i-j do
          statement(s)
```

Un petit corollaire

Théorème

L'aire d'un polygone simple discret finit toujours par ...,0 ou ...,5.

Merci !