Formalizzazione in HOL del Metodo Gosper/WZ e Applicazione alla Dimostrazione di Identità Binomiali

Giovanni Gherdovich
Relatore: Dott. Marco Maggesi

Curriculum Matematica Generale

26 aprile 2007

Theorem Provers Interattivi

Caratteristiche

- L'utente fornisce i passi della dimostrazione
- Libreria di teoremi integrata
- Procedure automatiche di deduzione

Si è usato il sistema HOL Light.

I Due Sistemi a Confronto

Computer Algebra Systems

- Potenza di calcolo
- Enunciati ambigui: $(x^2 - 1)/(x - 1) = x + 1$

Theorem Provers

- Semantica espressiva
- Risultati e dimostrazioni

Soluzioni e Certificati

Trovare la risposta è difficile, verificarla è semplice:

- Trovare divisori di polinomi (o numeri)
- Trovare MCD di polinomi (o numeri)
- Risolvere equazioni
- Trovare primitive

Approccio scettico all'oracolo esterno:

il CAS trova la risposta, il Theorem Prover la verifica.

Il Teorema WZ

H. Wilf e D. Zeilberger, 1990

Siano $F, G : \mathbb{N} \times \mathbb{Z} \to \mathbb{R}$ tali che

- $F(n+1,k) - F(n,k) = G(n,k+1) - G(n,k)$ [Telescopicità]
- $\lim_{k\to\pm\infty} G(n,k) = 0 \qquad \forall n \in \mathbb{N}$ [Bordo]
- $\sum_{k\in\mathbb{Z}} F(n,k) \quad \text{converge} \qquad \forall n \in \mathbb{N}$ [Convergenza]

Allora

$$\sum_{k\in\mathbb{Z}} F(n,k) = \text{ costante} \qquad \forall n \in \mathbb{N}$$

Dimostrazione.

$$\sum_k F(n+1,k) - \sum_k F(n,k) =$$

$$\sum_k \{F(n+1,k) - F(n,k)\} =$$

$$\sum_k \{G(n,k+1) - G(n,k)\} =$$

$$= 0$$

$\square$

Applicazione del Teorema: il Metodo Gosper/WZ

Il Metodo Gosper/WZ è una strategia non costruttiva per dimostrare identità della forma

$$\sum_{k \in \mathbb{Z}} f(n,k) = r(n)$$

- Trovare la funzione certificante $G(n,k)$.
- Verificare [Telescopicità], [Convergenza] e [Bordo]: la "versione breve" della dimostrazione.

Dal teorema, $\sum_k f(n,k)/r(n) = \texttt{costante}$.

- Verificare che l'identità vale per qualche n

L'Algoritmo di Gosper (1978)

Problema

Data $\{a_n\}$, esiste $\{S_n\}$ tale che $a_n = S_{n+1} - S_n$?

Soluzione, se $\{a_n\}$ ipergeometrica

Se $\frac{a_{n+1}}{a_n}$ è una funzione razionale di n, l'Algoritmo di Gosper dà una risposta completamente algoritmica.

Esempi di Identità Ipergeometriche

a cui il metodo si applica con successo.

- $\sum_k \binom{n}{k} = 2^n$
- $\sum_k \frac{\binom{n}{k}}{k!(a-k)!} = \frac{(n+a)!}{n!}$
- $\sum_k (-1)^k \frac{\binom{n}{k}}{\binom{k+a}{k}} = \frac{a}{n+a}$
- $\sum_k \binom{n}{k}^2 = \binom{2n}{n}$
- $\sum_k (-1)^k \binom{n}{k} \binom{2k}{k} 4^{n-k} = \binom{2n}{n}$
- $\sum_k (-1)^{n-k} \binom{2n}{k}^2 = \binom{2n}{n}$
- $\sum_k \binom{a}{k} \binom{n}{k} = \binom{n+a}{a}$

Coefficienti Binomiali a Parametri Interi

Definizione

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!} & \text{se } n \geq 0 \ \wedge \ k \geq 0 \ \wedge n \ \geq k \\ 0 & \text{altrimenti} \end{cases}$$

In HOL questa definizione non era disponibile. La si è ricavata da quella dei binomiali a parametri naturali, dimostrandone le usuali proprietà.

Il Metodo Gosper/WZ in Azione

$$\sum_k \binom{n}{k}^2 = \binom{2n}{n}$$

- Se $n < 0$ l'identità è valida
- Se $n \geq 0$, $F(n+1,k) - F(n,k) = G(n,k+1) - G(n,k)$ con
  - $F(n,k) = \binom{n}{k}^2 / \binom{2n}{n}$
  - $G(n,k) = -\frac{3n-2k+3}{2(2n+1)} \binom{n}{k-1}^2 / \binom{2n}{n}$

Osservazione

- [Convergenza] $\sum_k F(n,k)$ converge per ogni n, perchè $F(n,k)$ ha supporto finito in k
- [Bordo] $\lim_{k\to\pm\infty} G(n,k) = 0$ per ogni n, perchè $G(n,k)$ ha supporto finito in k

Mini-Teoria del Supporto Finito in HOL

Si sono dimostrati vari lemmi sulle funzioni a supporto finito in HOL, nello spirito del seguente:

```
⊢ ∀f:int->real a:int b:int.
     support (+) f (:int) ⊆ {i:int | a ≤ i ∧ i ≤ b}
       ⇒ sum {i:int | a ≤ i ∧ i ≤ b} f =
         sum (:int) f
```

Mini-Teoria del Supporto Finito in HOL

Dimostrazione in HOL del precedente lemma:

```
g `⊢ ∀f:int->real a:int b:int.
     support (+) f (:int) ⊆ {i:int | a ≤ i ∧ i ≤ b}
       ⇒ sum {i:int | a ≤ i ∧ i ≤ b} f = sum (:int) f`

e (REPEAT GEN_TAC THEN STRIP_TAC);;
e (ONCE_REWRITE_TAC [GSYM SUM_SUPPORT]);;
e (AP_THM_TAC THEN AP_TERM_TAC);;
e (MATCH_MP_TAC SUBSET_ANTISYM);;
e (CONJ_TAC);;
e (MATCH_MP_TAC SUPPORT_MONOTONIC);;
e (REWRITE_TAC [SUBSET; IN_UNIV]);;
e (SUBGOAL_THEN `!(f:int->real). support (+) f (:int) =
  support (+) f (support (+) f (:int))`
    (fun th -> ONCE_REWRITE_TAC [th])
  THENL [REWRITE_TAC [SUPPORT_SUPPORT]; ALL_TAC]);;
e (ASM_SIMP_TAC [SUPPORT_MONOTONIC]);;

let SUPPORT_SUBSET_INTSEG = top_thm();;
```

Il Secondo Membro Nullo

$$\sum_{k \in \mathbb{Z}} f(n,k) = r(n)$$

- $r(n) = 0$, verificare che $\sum_{k \in \mathbb{Z}} f(n,k) = 0$.
- $r(n) \neq 0$, dimostrare che $\sum_k \frac{f(n,k)}{r(n)} = 1$ per induzione su n.

Considerazione

Formalizzare questa casistica ha richiesto più lavoro delle aspettative.

Confronto tra gli Enunciati

Enunciato Standard

- Ipotesi di convergenza
- Condizione al bordo
- Ipotesi di telescopicità
- La tesi vale per un qualche n

Tesi

$\sum_{k\in\mathbb{Z}} F(n,k) = 1$

Enunciato Operativo

- Ipotesi di supporto finito
- Ipotesi di telescopicità
- Il supporto di $r(n)$ è un intervallo
- La tesi vale per un qualche n

Tesi

$\sum_{k\in\mathbb{Z}} f(n,k) = r(n)$

Dimostrazione del Teorema WZ in HOL

Digressione: se la teoria di base non è ben sviluppata, occorre molto, molto, molto lavoro in più.

Successioni con derivata discreta nulla in un sottoinsieme di $\mathbb{Z}$

```
⊢ ∀(P:int->bool) (f:int->real) (n0:int).
    ((∀n m. n ≤ m ∧ n ∈ P ∧ m ∈ P
          ⇒ {x | n ≤ x ∧ x ≤ m} ⊆ P) ∧
     P n0 ∧
     (∀n. P n ⇒ f (n + 1) - f n = 0))
      ⇒ (∀n. P n ⇒ f n = f n0)
```

Un'ipotesi di questo lemma necessita di essere suddivisa in casi.

Dimostrazione del Teorema WZ in HOL

Digressione: se la teoria di base non è ben sviluppata, occorre molto, molto, molto lavoro in più.

Questo dovrebbe essere semplice...

Semiretta, intervallo, tutto $\mathbb{Z}$ oppure $\emptyset$

```
⊢ ∀(P:int->bool).
      (∀n m. (n ≤ m ∧ P n ∧ P m ⇒ {x | n ≤ x ∧ x ≤ m} ⊂ P))
       ⇒
        ((∃a. ∃b. P = {(x:int) | a ≤ x ∧ x ≤ b} ∧ a ≤ b) ∨
        (∃c. P = {(x:int) | c ≤ x}) ∨
        (∃d. P = {(x:int) | x ≤ d}) ∨
        (∀(k:int). P k) ∨ (∀(k:int). ¬(P k)))
```

Dimostrazione del Teorema WZ in HOL

Digressione: se la teoria di base non è ben sviluppata, occorre molto, molto, molto lavoro in più.

...disponendo di una adeguata teoria degli insiemi di numeri interi.

sup di insiemi di numeri reali

$$\vdash \texttt{sup s} = \epsilon\texttt{a}.\ (\forall \texttt{x}.\ \texttt{x} \in \texttt{s} \Rightarrow \texttt{x} \leq \texttt{a}) \land \forall \texttt{b}.\ (\forall \texttt{x}.\ \texttt{x} \in \texttt{s} \Rightarrow \texttt{x} \leq \texttt{b}) \Rightarrow \texttt{a} \leq \texttt{b}$$

Massimo di insiemi di numeri interi

$$\vdash \texttt{max S} = \texttt{int\_of\_real (sup (IMAGE real\_of\_int S))}$$

Buona definizione: questo è davvero troppo tecnico

$$\vdash \forall \texttt{P}.\ \texttt{sup (IMAGE real\_of\_int P)} \in \texttt{IMAGE real\_of\_int P} \Rightarrow \texttt{real\_of\_int (max P) = (sup (IMAGE real\_of\_int P))}$$

Il Teorema WZ in HOL

```
∀F:int->int->real r:int->real.
     ((∀(n:int) m. (n ≤ m ∧
     n ∈ (support (+) (λi. r i) (:int)) ∧
     m ∈ (support (+) (λi. r i) (:int))) ⇒
     {x | n ≤ x ∧ x ≤ m} ⊆ (support (+) (λi. r i) (:int)))
∧
     (∃G:int->int->real. ∀n.
     (FINITE (support (+) (λk. (f n k)/(r n)) (:int))) ∧
     (FINITE (support (+) (λk. G n k) (:int))) ∧
     (¬(r n = 0) ⇒
     ∀k. (f (n + 1) k)/(r (n + 1)) - (f n k)/(r n) = G n (k + 1) - (G n k)))
∧
     (∀n. r n = 0 ⇒ (sum (:int) (λk. f n k) = r n))
∧
     (∃m:int. (sum (:int) (λk. f m k) =  r m) ∧ ¬(r m = 0))
  ⇒ (sum (:int) (λk. f n k) = r n)
```

Semplificare i Binomiali

Riscritture condizionali

Top Step

$$\binom{n+1}{k} = \begin{cases} 0 & \text{se } k = n+1 \\ & \text{ e } n+1 < 0 \\ 1 & \text{se } k = n+1 \\ & \text{ e } n+1 \geq 0 \\ \frac{n+1}{n+1-k}\binom{n}{k} & \text{altrimenti} \end{cases}$$

Top Backstep

$$\binom{n-1}{k} = \begin{cases} 0 & \text{se } n = 0 \\ \frac{n-k}{n}\binom{n}{k} & \text{altrimenti} \end{cases}$$

Bottom Step

$$\binom{n}{k+1} = \begin{cases} 0 & \text{se } k+1 = 0 \\ & \text{ e } n < 0 \\ 1 & \text{se } k+1 = 0 \\ & \text{ e } n \geq 0 \\ \frac{n-k}{k+1}\binom{n}{k} & \text{altrimenti} \end{cases}$$

Bottom Backstep

$$\binom{n}{k-1} = \begin{cases} 0 & \text{se } k = n+1 \\ & \text{ e } n < 0 \\ 1 & \text{se } k = n+1 \\ & \text{ e } n \geq 0 \\ \frac{k}{n+1-k}\binom{n}{k} & \text{altrimenti} \end{cases}$$

Semplificare i Binomiali

Riscritture condizionali

‘$\binom{(a+b)+1}{k}$ = qualcosa‘

Applicando la riscrittura “Top Step” si ottengono tre subgoals:

```
val it : goalstack = 3 subgoals (3 total)

0 [‘k = (a + b) + 1‘]
1 [‘0 ≤ (a + b) + 1]
‘1 = qualcosa‘

0 [‘k = (a + b) + &1‘]
1 [‘¬(0 ≤ (a + b) + 1)‘]
‘0 = qualcosa‘

0 [‘¬(k = (a + b) + &1)‘]
1 [‘¬((a + b) + 1 - k = 0)‘]
```

‘$\frac{a+b+1}{a+b+1-k}\binom{a+b}{k}$ = qualcosa‘

L'aiuto dall'esterno

Il Computer Algebra System Maxima trova che la funzione certificante è $G(n,k) = \frac{-(3n-2k+3)\binom{n}{k-1}^2}{2(2n+1)\binom{2n}{n}}$

Ipotesi di supporto finito al posto di [Convergenza]

$$\text{`FINITE (support (+) (}\lambda\text{k. } \frac{\binom{n}{k}^2}{\binom{2n}{n}}\text{) (:int))`}$$

Ipotesi di supporto finito al posto di [Bordo]

$$\text{`FINITE (support (+) (}\lambda\text{k. } \frac{-(3n-2k+3)\binom{n}{k-1}^2}{2(2n+1)\ \binom{2n}{n}}\text{) (:int))`}$$

Dimostrazione di $\sum_k \binom{n}{k}^2 = \binom{2n}{n}$ in HOL

La verifica del certificato

Il supporto del secondo membro è un intervallo

$$
\begin{array}{l}
\ \ 0\ [\texttt{`n} \le \texttt{m`}] \\
\ \ 1\ [\texttt{`n} \in \texttt{support (+) (}\lambda\texttt{i. (}\lambda\texttt{j. } \binom{2j}{j}\texttt{) i) (:int)`}] \\
\ \ 2\ [\texttt{`m} \in \texttt{support (+) (}\lambda\texttt{i. (}\lambda\texttt{j. } \binom{2j}{j}\texttt{) i) (:int)`}] \\
\texttt{`}\{\texttt{x} \mid \texttt{n} \le \texttt{x} \wedge \texttt{x} \le \texttt{m}\} \subseteq \texttt{support (+) (}\lambda\texttt{i. (}\lambda\texttt{j. } \binom{2j}{j}\texttt{) i) (:int)`}
\end{array}
$$

L'identità vale se il secondo membro è nullo

$$
\begin{array}{l}
\ \ 0\ [\texttt{`(}\lambda\texttt{j. } \binom{2j}{j}\texttt{) n = 0`}] \\
\texttt{`sum (:int) (}\lambda\texttt{k. (}\lambda\texttt{n k. } \binom{n}{k}^2\texttt{) n k) = (}\lambda\texttt{j. } \binom{2j}{j}\texttt{) n`}
\end{array}
$$

L'indentità vale per qualche n

$$
\begin{array}{l}
\texttt{`}\exists\texttt{m. sum (:int) (}\lambda\texttt{k. (}\lambda\texttt{n k. } \binom{n}{k}^2\texttt{) m k) = (}\lambda\texttt{j. } \binom{2j}{j}\texttt{) m} \wedge \\
\qquad \neg\texttt{((}\lambda\texttt{j. } \binom{2j}{j}\texttt{ j)) m = 0)`}
\end{array}
$$

Ipotesi di telescopicità

$$`\neg(\binom{2n}{n} = 0) \Rightarrow$$
$$\forall k.\ \frac{\binom{n+1}{k}^2}{\binom{2n+1+1}{n+1}} - \frac{\binom{n}{k}^2}{\binom{2n}{n}} = \frac{-(3n-2(k+1)+3)\binom{n}{k}^2}{2(2n+1)\binom{2n}{n}} - \frac{-(3n-2k+3)\binom{n}{k-1}^2}{2(2n+1)\binom{2n}{n}}`$$

1. Convertire l'ipotesi $r(n) \neq 0$ in condizioni esplicite su n.
2. Applicare le riscritture condizionali eliminando i subgoals inconsistenti.
3. Usare le procedure automatiche per l'aritmetica.

Dimostrazione di $\sum_k \binom{n}{k}^2 = \binom{2n}{n}$ in HOL

Ipotesi di telescopicità: due tipi di subgoals

Primo tipo: sono presenti tutti i coefficienti binomiali

```
0 [‘¬(¬(0 ≤ 2 * n) ∨ ¬(0 ≤ n) ∨ 2 * n < n)‘]      4 [‘¬(n + 1 - k = 0)‘]
1 [‘¬(n + 1 = (2 * n + 1) + 1)‘]                    5 [‘¬(n + 1 = 2 * n + 1)‘]
2 [‘¬((2 * n + 1) + 1 - (n + 1) = 0)‘]              6 [‘¬((2 * n) + 1 - (n + 1) = 0)‘]
3 [‘¬(k = n + 1)‘]                                  7 [‘¬(n + 1 = 0)‘]
```

$$‘\ \frac{\left(\frac{n+1}{n+1-k}\binom{n}{k}\right)^2}{\frac{2n+1+1}{2n+1+1-(n+1)}\,\frac{2n+1}{2n+1-(n+1)}\,\frac{2n-n}{n+1}\binom{2n}{n}} - \frac{\binom{n}{k}^2}{\binom{2n}{n}} = \frac{-(3n-2k+1)\binom{n}{k}^2}{2(2n+1)\binom{2n}{n}} - \frac{-(3n-2k+3)\left(\frac{k}{n+1-k}\binom{n}{k}\right)^2}{2(2n+1)\binom{2n}{n}}\ ‘$$

Da funzioni razionali a funzioni polinomiali

```
⊢ ∀a b c d e f g h.
        ¬(b = 0) ∧ ¬(d = 0) ∧ ¬(f = 0) ∧ ¬(h = 0) ∧
        (a * d - b * c) * f * h = (e * h - g * f) * b * d
        ⇒  a / b - c / d = e / f - g / h
```

Dimostrazione di $\sum_k \binom{n}{k}^2 = \binom{2n}{n}$ in HOL

Ipotesi di telescopicità: due tipi di subgoals

Secondo tipo: alcuni binomiali sono sostituiti da 0 oppure 1

```
0 [`¬(¬(0 ≤ 2 * n) ∨ ¬(0 ≤ n) ∨ 2 * n < n)`]
1 [`¬(n + 1 = (2 * n + 1) + 1)`]
2 [`¬((2 * n + 1) + 1 - (n + 1) = 0)`]
3 [`k = n + 1`]
4 [`0 ≤ n + 1`]
5 [`n + 1 = 2 * n + 1`]
6 [`0 ≤ 2 * n + 1`]
7 [`0 ≤ n`]
```

$$`\frac{1^2}{\frac{(2n+1)+1}{(2n+1)+1-(n+1)} \cdot 1} - \frac{\binom{n}{k}^2}{\binom{2n}{n}} = \frac{-(3n-2(k+1)+3)\binom{n}{k}^2}{2(2n+1)\binom{2n}{n}} - \frac{-(3n-2k+3) \cdot 1^2}{2(2n+1)\binom{2n}{n}}`$$

Da funzioni razionali a funzioni polinomiali

```
⊢ ∀a b c d e f g h.
        ¬(b = 0) ∧ ¬(d = 0) ∧ ¬(f = 0) ∧ ¬(h = 0) ∧
        (a * d - b * c) * f * h = (e * h - g * f) * b * d
        ⇒  a / b - c / d = e / f - g / h
```

THEN, REPEAT REWRITE e