Sulla teoria di $\mathbb{Z}$ in $L = \{+, <\}$

Andrea Vaccaro

1 Premesse

Si consideri il linguaggio $L = \{+, <\}$, e in esso la teoria degli interi $\text{Th}(\mathbb{Z}, +, <)$. Nel presente documento si fornirà un'assiomatizzazione ricorsiva di tale teoria, e lo studio dell'eliminazione dei quantificatori in una sua espansione, in un linguaggio L' che verrà definito più avanti.

Si consideri allora la teoria T cosituita dai seguenti assiomi:

- ordini totali discreti
- gruppi abeliani
- $\forall xyz\left(x < y \to x + z < y + z\right)$
- per ogni $n \geq 2 \in \mathbb{N}$ un assioma di questo tipo:

$$\forall x \exists mz\,(x = m + nz \wedge 0 \leq m < n)$$

In questo schema di assiomi sono state utilizzate diverse abbreviazioni. Con nz si intende l'oggetto z sommato n volte; con 0 si intende l'elemento neutro derivante dagli assiomi della teoria dei gruppi (e dunque definibile nel linguaggio L); infine, gli assiomi degli ordini discreti ci consentono di definire il successore, e dunque in questo caso specifico il successore dell'elemento neutro (che potremmo chiamare ad esempio 1). Con n si intende tale elemento sommato n volte. Da qui in avanti, per comodità, un generico elemento $n \in \mathbb{Z}$ rappresenterà la somma di n volte 1 o del suo opposto, a seconda del segno.

A questo punto consideriamo il linguaggio $L' = \{+, <, -, 0, 1\} \cup \{\equiv_n\}_{n \geq 2 \in \mathbb{N}}$, dove 0 e 1 sono due simboli di costante, $-$ è un simbolo di funzione unaria, e ognuno dei $\equiv_n$ rappresenta un simbolo di relazione. Possiamo allora estendere T a una nuova teoria T' che contenga anche i seguenti assiomi:

- $\forall x\left(x = 0 \leftrightarrow \forall y\left(x + y = y\right)\right)$
- $\forall x\left(x = 1 \leftrightarrow 0 < x \wedge \nexists y\left(0 < y < x\right)\right)$
- $\forall xy\left(x = -y \leftrightarrow x + y = 0\right)$
- $\forall xy\left(x \equiv_n y \leftrightarrow \exists z\left(x - y = nz\right)\right)$

Notare come in L', $n \in \mathbb{Z}$ sia un termine chiuso.

É chiaro che ogni modello M di T può essere espanso ad un modello di T' in modo unico, semplicemente interpretando come definizioni su M tali assiomi; viceversa ogni modello di T' può essere ristretto ad uno di T.

A questo punto l'idea è quella di mostrare che T' ammette l'eliminazione dei quantificatori.

Diamo per buono tale fatto, per il momento. É facile verificare che ogni modello M di T' ammette una sottostruttura isomorfa a $\mathbb{Z}$. Nella fattispecie, tale sottostruttura è data da $< 0, 1 >_M$. L'isomorfismo, come si può immaginare, è:

$$\phi : \mathbb{Z} \to < 0, 1 >_M$$
$$\phi\left(n^{\mathbb{Z}}\right) = n^M$$

Questo fatto, grazie all'eliminazione dei quantificatori, ci garantisce la completezza di T'.

Dalla completezza di T' segue anche facilmente la completezza di T. Siano infatti M ed N tali che $M, N \models T$, e sia ϕ una $L-$formula, e valga $M \models_L \phi$. A questo punto espandiamo M ed N a L', e poiché ϕ è anche una $L'-$formula, si può ancora dire che $M \models_{L'} \phi$. Per completezza di T', $N \models_{L'} \phi$, e perciò $N \models_L \phi$. In modo analogo vale anche il viceversa, dunque $M \equiv N$, pertanto T è completa (per una dimostrazione rigorosa del fatto che $M \models_L \phi \iff M \models_{L'} \phi$, quando ϕ sia una $L-$formula, è sufficiente lavorare per induzione sulle formule).

Dal momento che $\mathbb{Z}$, con le classiche interpretazioni di $+$ e $<$, è un modello di T, si ricava che $T = \mathrm{Th}(\mathbb{Z}, +, <)$.

Tutto si riduce dunque a mostrare che T' ammette l'eliminazione dei quantificatori.

2 Eliminazione dei Quantificatori di T'

Per mostrare che in T' vale l'eliminazione dei quantificatori, verrà considerata una $L'-$formula primitiva $\phi(\mathbf{x})$, e verrà dimostrato che per ogni $M, N \models T'$, e per ogni $f : \mathrm{dom} f \to \mathrm{Im} f$ isomorifismo parziale finito da M a N vale che per ogni $\mathbf{a} \in \mathrm{dom} f$

$$M \models \phi(\mathbf{a}) \iff N \models \phi(f\mathbf{a})$$

Si ha dunque che $\phi(\mathbf{x}) \equiv \exists y \psi(\mathbf{x}, y)$, dove ψ è congiunzione di atomiche e negazioni di atomiche.

Scopo dunque di questa sezione, per verificare l'eliminazione dei quantificatori in T', sarà quello di verificare che se si può trovare in M un a tale che $\psi(a_1, \ldots, a_n, a)$ con gli $a_i \in \mathrm{dom} f$, si può anche trovare in N un b tale che valga $\psi(f a_1, \ldots, f a_n, b)$, e viceversa (verrà mostrato un solo verso, per l'altro basterà ripercorrere la dimostrazione sostituendo a f l'inversa f^{-1}).

Le formule atomiche in $\psi(\mathbf{a}, a)$ sono di 3 tipi:

$$n' + \sum_{i=1}^{k} \pm a_i = na$$

$$m' + \sum_{i=1}^{k} \pm a'_i > ma$$

$$v' + \sum_{i=1}^{k} \pm a''_i \equiv_l va$$

ove gli a_i, a'_i, a''_i sono componenti di $\mathbf{a}$.

Nella dimostrazione che seguirà si potrà considerare, senza perdere di generalità, la ψ senza negazioni di atomiche. La negazione di uguaglianza può infatti essere sostituita dalla disgiunzione di due disuguaglianze, la negazione di una disuguaglianza può essere invece sostiuita dalla disgiunzione di un'uguaglianza e di un'altra disuguaglianza (è immediato verificare che il simbolo di $<$ si comporta rispetto alla funzione $-$ come ci si aspetta, ovvero si gira). Infine, la negazione di una congruenza modulo l può essere sostiuita da una disgiunzione di $l-1$ congruenze modulo l (dove compaiono tutti gli m fra 0 e $l-1$ escluso quello della disuguaglianza stessa). A questo punto si può distribuire l'esistenziale sulle disgiuntive e ragionare per induzione.

In realtà la ψ può essere ulteriormente semplificata, nel caso vi siano uguaglianze o disuguaglianze. Immaginiamo che in ψ vi sia una congiunzione di uguaglianze

$$\bigwedge_{h=1}^{l} n'_h + \sum_i \pm a_{h,i} = n_h a$$

con tutti gli $n_h \neq 0$ (quelle dove $n_h = 0$ potranno poi essere portate fuori dal quantificatore, e dunque verificate in N per le proprietà di isomorfismo). É immediato verificare che in T' si dimostra, dato $m \neq 0$ in $\mathbb{Z}$, $\forall xy\left(x = y \leftrightarrow mx = my\right)$. Se allora $N = \prod_h n_h$ e $N_i = \prod_{h \neq i} n_h$, l'equazione $N_1\left(n'_1 + \sum_i \pm a_{1,i}\right) = Na$ è equivalente a tutte le altre della congiunzione. Da un lato infatti la prima uguaglianza della congiunzione implica tale uguaglianza, dall'altro, poiché vale

$$N_j \left(n'_j + \sum_i \pm a_{j,i} \right) = N_k \left(n'_k + \sum_i \pm a_{k,i} \right) \quad \forall 1 \leq j, k \leq l$$

relazione ricavata grazie al fatto che $M \models \exists x \psi(\mathbf{a}, x)$, si ha che $N_j \left(n'_j + \sum_i \pm a_{j,i} \right) = Na$ per ogni j da 1 a l, da queste si possono poi riottenere le uguaglianze della congiunzione di partenza.

In buona sostanza, verificata la prima uguaglianza, venendo in questo modo a fissato in modo univoco, verificherà anche le altre.

Quanto ottenuto consente di poter considerare in ψ, senza perdere di generalità, al più un'unica uguaglianza.

In modo analogo ci si può ridurre a due disuguaglianze (sempre che in ψ ve ne siano). Si immagini che in ψ vi siano le seguenti:

$$\bigwedge_{p=1}^{q} m'_p + \sum_i \pm a'_{p,i} > m_p a \wedge \bigwedge_{s=1}^{t} m'_s + \sum_i \pm a'_{s,i} > m_s a$$

dove gli m_p sono positivi e gli m_s negativi (ovvero somma di opposti di a)(di nuovo i casi con $m_i = 0$ non forniscono vere informazioni su a, dunque sul b che dovremo cercare). Possiamo considerare anche m_s positivi a patto di cambiare segno di disuguaglianza e cambiare segno al termine a sinistra (cosa che a livello notazionale, per comodità, non condurrà a nessuna modifica). Si può verificare in modo semplice che, dato n intero positivo, in T' si verifica che $\forall xy (x < y \leftrightarrow nx < ny)$.

Ci restringiamo ora al primo blocco di disuguaglianze. Ponendo $M = \prod_h m_h$ e $M_i = \prod_{h \neq i} m_h$, per ogni j si verifica che

$$M_j \left(m'_j + \sum_i \pm a'_{j,i} \right) > Ma$$

prendendo allora il minimo degli $M_j \left(m'_j + \sum_i \pm a'_{j,i} \right)$, e supponendo sia quello con indice 1, la formula

$$M_1 \left(m'_1 + \sum_i \pm a'_{1,i} \right) > Ma$$

è equivalente al primo blocco di congiunzioni. Da un lato questa formula è implicata dalla prima disuguaglianza del blocco, dall'altro essa implica per tutti gli altri j fra 2 e t, $M_j \left(m'_j + \sum_i \pm a'_{j,i} \right) > Ma$ e dunque le disuguaglianze presenti in ψ; analogo discorso si può fare col secondo blocco, ragionando però col massimo dei $\tilde{M}_k \left(m'_k + \sum_i \pm a'_{k,i} \right)$. Ci si può di nuovo ridurre ad un'unica disuguaglianza

$$\tilde{M}_1 \left(m'_1 + \sum_i \pm a'_{1,i} \right) < \tilde{M} a$$

In conclusione, ponendo $\hat{M} = M\tilde{M}$, tutte le disuguaglianze sono ridotte a

$$M\tilde{M}_1 \left(m'_1 + \sum_i \pm a'_{1,i} \right) < \hat{M} a < \tilde{M} M_1 \left(m'_1 + \sum_i \pm a'_{1,i} \right)$$

Chiaro che in mancanza di uno dei due blocchi di disuguaglianze, avremo rispettivamente solo la prima o la seconda.

In definitiva, se in ψ dovessero comparire uguaglianze e disuguaglianze, si potrà riscrivere $\psi(a_1, \ldots, a_n, a)$ in modo equivalente come:

$$n' + \sum_i \pm a_i = na \wedge m' + \sum_i \pm a'_i < ma < m'' + \sum_i \pm a''_i \wedge \bigwedge_{h=1}^{k} v'_h + \sum_i \pm a'''_{h,i} \equiv_{l_h} v_h a$$

Concentriamoci ora sul trovare un $b \in N$ tale per cui $N \models \psi(b_1, \ldots, b_n, b)$, dove $b_i = f a_i$. Ragioniamo per casi su ψ.

2.1 Congruenze

Se ψ è congiunzione di sole congruenze, allora sarà una formula di questa forma:

$$\bigwedge_h^k v'_h + \sum_i \pm a'''_{h,i} \equiv_{l_h} v_h a$$

Consideriamo allora a che in M verifichi tale congruenze. Sia $F = \text{mcm}(l_h)$, e sia $0 \le G < F$ tale che $a \equiv_F G$. É chiaro che $a \equiv_{l_h} G$ per ogni h. Se si considera allora nel modello N il valore G (ovviamente si sta considerando rispettivamente G^M e G^N; da qui in avanti la distinzione non verrà specificata, poiché evidente dal contesto), ponendo $b = G$ si ottiene un elemento di N che verifica il sistema di congruenze, perciò si ottiene $N \models \psi(b_1, \dots b_n, b)$, come richiesto. Notare che la scelta di b è unica modulo F.

2.2 Disuguaglianze

Supponiamo ora invece che ψ si congiunzione di sole disuguaglianze. Si è detto che ci si può ridurre solo a due di esse. Supponiamo in un primo caso che sia solo una ovvero $\psi(a_1, \dots, a_n, a) \equiv m' + \sum_i \pm a''_i > ma$. Per comodità verrà indicato $B = m' + \sum_i \pm a''_i$. Per trovare il corrispondete b in N si proceda come segue: si prenda il primo valore più grande di $m' + \sum_i \pm b''_i$ conguro a zero modulo m (tale valore certamente esiste, si parta da fB, sommando 1 un numero sufficiente di volte (finito in quanto minore di $m+1$) si troverà il valore cercato.). Sia tale valore C. Poiché è congruo a zero modulo m, esiste in N un b tale che $C = \sum_m b$. Tale b è il valore cercato. Si proceda in modo analogo in presenza di una sola disugualglianza con $<$.

Supponiamo ora sia $\psi(a_1, \dots, a_n, a) \equiv A < ma < B$, con B definito come sopra e $A = m' + \sum_i \pm a'_i$. Si conclude nel momento in cui si trova un elemento di N, diciamo C, che sia tale da essere

$$fA < C < fB$$

$$C \equiv_m 0$$

Ciò che si ricava è che, per un opportuno $0 < k \le m$, $A + k$ è congruo a zero modulo m ed è tale da verificare $A < A + k < B$, perciò anche la sua immagine mediante f rispetterà tali proprietà rispetto a fA ed fB, perciò sarà il valore cercato (b sarà poi il valore tale che $\sum_m b = C$). Ma come mai tale k esiste? Il primo valore conguro a zero modulo m in (A, B) è di sicuro fra $A+1, \dots, A+m$; se in (A, B) non vi fosse tale $A + k$, ovvero se fosse maggiore di B, allora non vi potrebbero essere altri valori congrui a zero modulo m in (A, B), contro l'ipotesi $ma \in (A, B)$.

2.3 Disuguaglianze e congruenze

A questo punto si supponga di avere ψ equivalente a un sistema di congruenze e una sola disuguaglianza, diciamo $A < ma$. Ricordando che la soluzione trovata nella sezione delle congruenze era unica modulo F, sarà sufficiente trovare un valore in N congruo a G modulo F che sia abbastanza grande. Si può sempre trovare un valore congruo a G modulo F maggiore di $\max(0, fA)$, grazie agli assiomi degli ordini lineari discreti. Dato allora tale valore b, è chiaro che questi verifichi sia la congruenza che $mb > fA$ (fondamentale qui che $b > 0$). In modo analogo si può trovare b se la disuguaglianza fosse $B > ma$, cercando in N un valore congruo a G modulo F minore di $\min(0, fB)$.

Supponiamo ora invece di avere delle disuguaglianze che impongano $A < ma < B$. Vi sono due casi: Il primo, in cui la distanza fra A e B è infinita; in questo caso, poiché f al solito è isomorfismo parziale, anche la distanza fra fA ed fB è infinita (ovvero $fB - fA > h$ per ogni $h \in \mathbb{Z}$). Nella sezione sulle disuguaglianze, quando si aveva a che fare con un intervallo (fA, fB) il b trovato tale che $mb \in (fA, fB)$ era in buona sostanza il primo che andava bene, in particolare tale che mb fosse ad una distanza finita da fA. Se vale che $b \equiv_F G$, tale b va già bene. In caso contrario, sommando a b il valore 1 un numero sufficiente (ma finito) di volte, diciamo t, si otterrà un $b' \equiv_F G$. A questo punto, $mb' = mb + mt$ è ancora in (fA, fB), in quanto ad una distanza finita da mb, a sua volta a distanza finita da fA. Perciò b' verificherà le richieste poste da ψ.

Nel caso in cui (A, B) sia di lunghezza finita, varrà che $B = A + h$, pertanto anche $fB = fA + h$. Si avrà allora che $ma = A + k$ con $k < h$. Ma allora si può cercare il b tale che $mb = fA + k$. In questo modo stiamo di fatto aggiungendo un'uguaglianza alla ψ; rimandiamo allora alle prossime sezioni la verifica dell'esistenza di un b adatto ("Uguaglianza, disuguaglianze e congruenze").

2.4 Uguaglianza

Come già detto, se in ψ compaiono solo uguaglianze, è possibile ridursi ad una sola uguaglianza equivalente a ψ. Supponiamo sia allora

$$n' + \sum_i \pm a_i = na$$

Ciò siginifica che

$$n' + \sum_i \pm a_i \equiv_n 0$$

Visto che f è isomorfismo parziale, vale anche

$$n' + \sum_i \pm b_i \equiv_n 0$$

perciò esiste b tale che

$$n' + \sum_i \pm b_i = nb$$

Questo è l'elemento di N cercato.

2.5 Uguaglianza e disuguaglianze

Fissata l'uguaglianza, si è già trovato un b in N. Mostriamo ora che rispetta anche le due eventuali disuguaglianze. Sia l'uguaglianza

$$n' + \sum_i \pm a_i = na$$

dove, senza perdere di generalità, si suppone n positivo, e una disuguaglianza

$$m'' + \sum_i \pm a''_i > ma$$

Grazie a fatti dimostrati in precedenza e grazie al fatto che f è isomorfismo parziale, si verifica che

$$m'' + \sum_i \pm a''_i > ma \iff n\left(m'' + \sum_i \pm a''_i\right) > mna \iff n\left(m'' + \sum_i \pm a''_i\right) > m\left(n' + \sum_i \pm a_i\right)$$

$$n\left(m'' + \sum_i \pm a''_i\right) > m\left(n' + \sum_i \pm a_i\right) \iff n\left(m'' + \sum_i \pm b''_i\right) > m\left(n' + \sum_i \pm b_i\right) \iff n\left(m'' + \sum_i \pm b''_i\right) > mnb$$

$$n\left(m'' + \sum_i \pm b''_i\right) > mnb \iff m'' + \sum_i \pm b''_i > mb$$

Stesso procedimento con l'altra disuguaglianza.

2.6 Uguaglianza, disuguaglianze e congrenze

Come già visto, il b trovato con l'uguaglianza, risolve le eventuali disuguaglianze. Verrà mostrato ora che risolverà anche tutte le congruenze in ψ. Il problema è risolto se anche $b \equiv_F G$. In modo improprio qui di seguito verrà detto che un elemento di M è congruo modulo un certo t ad uno di N; tale notazione ovviamente di per sè non ha senso, sarà per noi un'abbreviazione per dire che sono congrui entrambi all'$n-$simo successore dello zero, rispettivamente di M ed N. Ad esempio, l'ugualgianza di ψ, grazie al fatto che f è isomorfismo parziale, ci consente di dire, che $na \equiv_F nG \equiv_F nb$.

Poiché si sa già che $a \equiv_F G$, si ricava che

$$n' + \sum_i \pm a_i = na = n(G + Fx) = nG + nFx$$

ovvero

$$n' + \sum_i \pm a_i \equiv_{nF} nG$$

ciò garantisce che

$$nb = n' + \sum_i \pm b_i \equiv_{nF} nG$$

Dal momento che $G < F$ e poiché si può sempre supporre $n > 0$, vale che $nG < nF$.

Per gli assiomi si può supporre esista $G' < F$ tale che $b \equiv_F G'$. Si ottiene allora:

$$nG \equiv_{nF} nb \equiv_{nF} nG'$$

con sia G che G' compresi fra 0 (debolmente) e F (strettamente). Se fosse $G \neq G'$, sarebbe facile ricavare un assurdo. Sia infatti $0 \leq G < G' < F$; poiché $nG \equiv_{nF} nG'$ allora $n\left(G' - G\right) = nFx$, e dunque $G' - G = Fx$ con $x > 0$ (segue da $G' > G$), perciò vale anche che $x \geq 1$, che implica $Fx \geq F$, cioè $G' - G \geq F$, e dunque $G' \geq F + G \geq F$, assurdo per ipotesi su G'.