Daniele Mundici

La Logica dei Poliedri

Bollettino dell'Unione Matematica Italiana, Serie 9, Vol. **1** (2008), n.2, p. 455–474.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_2008_9_1_2_455_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana,
2008.

Bollettino U. M. I.
(9) **I** (2008), 455-474

La Logica dei Poliedri (*)

DANIELE MUNDICI

Abstract. – *We describe the deep relationship between rational polyhedra, weighted abstract simplicial complexes, and finitely presented MV-algebras—the algebras of finitely axiomatizable theories in Łukasiewicz infinite-valued logic. Combining Alexander's classical stellar machinery with the solution, by Włodarczyk and Morelli, of the weak Oda conjecture on toric varieties, we shall present several results involving classification, measurability, dissectability, and computability.*

1. – Antefatto: Poliedri e complessi astratti

Per $0 \leq m \leq n$, un *m-simplesso* nello spazio euclideo $\mathbb{R}^n$ è la chiusura convessa $T = \text{conv}(w_0, \ldots, w_m)$ di $m + 1$ punti in $\mathbb{R}^n$ affinemente indipendenti. I *vertici* $w_0, \ldots, w_m$ sono univocamente individuati da T. Seguendo [51], un *poliedro convesso* C in $\mathbb{R}^n$ è un insieme compatto non vuoto esprimibile come chiusura convessa di un insieme finito di punti in $\mathbb{R}^n$.

Per *poliedro* $P \subseteq \mathbb{R}^n$ intendiamo un'unione finita di poliedri convessi in $\mathbb{R}^n$. In altre parole P è l'unione di un numero finito di simplessi in $\mathbb{R}^n$.

Un *complesso simpliciale astratto* è una coppia $(\mathcal{V}, \Sigma)$ ove $\mathcal{V} = \{u_1, \ldots, u_n\}$ è un insieme finito non vuoto, e Σ è una collezione di sottinsiemi di $\mathcal{V}$ la cui unione coincide con $\mathcal{V}$, tale che ogni sottinsieme di un membro di Σ è anch'esso un membro di Σ. Indicando con $e_1, \ldots, e_n$ i vettori di base standard di $\mathbb{R}^n$, la *realizzazione geometrica* di K è l'insieme Δ_K di tutti i simplessi $T = \text{conv}(e_{i(0)}, \ldots, e_{i(m)}) \subseteq \mathbb{R}^n$, per $m = 0, \ldots, n$, tali che $\{u_{i(0)}, \ldots, u_{i(m)}\}$ appartiene a Σ. Denotiamo con $|\Delta_K|$ l'unione (punto per punto) di tutti i simplessi di Δ_K. Per ogni insieme $\emptyset \neq A \in \Sigma$ ed elemento $a \notin \mathcal{V}$ il complesso simpliciale astratto $(A, a)(\mathcal{V}, \Sigma)$ si ottiene eliminando ogni $C \in \Sigma$ tale che $C \supseteq A$, e sostituendolo con tutti gli insiemi della forma $F \cup \{a\}$, ove F è ogni possibile sottinsieme di C che non contiene A. Seguendo [1, p. 298] diciamo che $(A, a)(\mathcal{V}, \Sigma)$ è una *suddivisione semplice* di $(\mathcal{V}, \Sigma)$. Due complessi simpliciali astratti sono *equivalenti* se sono collegati da un cammino di suddivisioni semplici e loro inverse.

(*) Conferenza Generale tenuta a Bari il 29 settembre 2007 in occasione del XVIII Congresso dell'Unione Matematica Italiana.

Newman e Alexander dimostrarono [1, 15:1], [18, 4.5]:

TEOREMA 1.1. – *La funzione* $K \mapsto |\Delta_K|$ *determina una corrispondenza biunivoca tra le classi di equivalenza dei complessi simpliciali astratti e le classi di PL-omeomorfismo dei poliedri.*

Tradizionalmente, per ogni relazione di equivalenza definita su oggetti *finitamente presentati* si pone il problema di riconoscere l'equivalenza di due oggetti arbitrari mediante una procedura che termini in un numero finito di passi. In particolare per i complessi simpliciali astratti un corollario del Teorema 1.2 di Markov (che sarà enunciato nelle prossime righe) alla luce del Teorema 1.1 stabilisce che *non esiste una procedura che in un numero finito di passi decida se due complessi simpliciali astratti sono o no equivalenti.* Per una definizione rigorosa di "procedura che termina in numero finito di passi", qui assolutamente necessaria, possiamo indifferentemente pensare a una macchina di Turing, a una funzione ricorsiva, o a un programma di computer, [20] (1). In realtà Markov dimostrò l'irriconoscibilità dei poliedri—ma per enunciare il suo teorema dobbiamo tener conto del fatto che in generale un poliedro porta con sé una quantità infinita di informazione, e non può quindi essere dato in input al computer. E allora diciamo che un poliedro $Q \subseteq \mathbb{R}^n$ è *razionale* se Q è un'unione finita di chiusure convesse di insiemi finiti di punti razionali. Il passaggio dai poliedri ai poliedri razionali è un dettaglio irrilevante, visto che ogni poliedro P può essere trasformato in un poliedro razionale P' PL-omeomorfo a P mediante un piccolissimo spostamento dei suoi vertici: questo P' può essere presentato come un elenco finito di simboli. Markov dimostrò questo famoso teorema, [5]:

TEOREMA 1.2. – *Non esiste una procedura che in un numero finito di passi riconosca se due poliedri razionali sono PL-omeomorfi. Quindi non è possibile una classificazione dei poliedri mediante invarianti che siano completi per PL-omeomorfismo ed effettivamente calcolabili.*

2. – Poliedri razionali, complessi pesati, logica di Łukasiewicz.

Di fronte a un risultato negativo della portata del Teorema 1.2 chi voglia assegnare invarianti ai poliedri razionali è naturalmente portato a introdurre raffinamenti della nozione di "equivalenza tra poliedri" e della nozione di "com-

(1) La *definizione* di "procedura che termina in numero finito di passi", o "procedura effettiva", è un importante risultato matematico del secolo scorso, scaturito dall'esigenza di rispondere al Problema della Decisione di Hilbert, sviluppato nella Macchina di Turing Universale, e progressivamente materializzato nel Computer.

plesso simpliciale astratto”, che tengano conto della razionalità dei vertici–prerequisito ineludibile per ogni costruzione effettiva sui poliedri.

A questo proposito, dati due poliedri razionali $P \subseteq \mathbb{R}^n$ e $Q \subseteq \mathbb{R}^m$ scriviamo $P \cong_{\mathbb{Z}} Q$, e diciamo che P è $\mathbb{Z}$*-omeomorfo* a Q, se esiste un PL-omeomorfismo η di P su Q (sempre con un numero finito di pezzi lineari $\varepsilon_1, \ldots, \varepsilon_k$) tale che ogni pezzo lineare di η e di η^{-1} abbia coefficienti interi. Dunque per ogni $x \in P$ esiste un $i = 1, \ldots, k$ tale che $\eta(x) = \varepsilon_i(x)$. Già nel caso $P = [0,1]^2$ il gruppo degli $\mathbb{Z}$-omeomorfismi di P su P ha interessanti proprietà ergodiche [40, 42].

Contestualmente, per una classificazione combinatoria dei poliedri razionali a meno di $\mathbb{Z}$-omeomorfismo, chiamiamo complesso simpliciale astratto *pesato* una tripletta $K = (\mathcal{V}, \Sigma, \omega)$ ove $(\mathcal{V}, \Sigma)$ è un complesso simpliciale astratto, e ω è una *funzione peso* $\omega: \mathcal{V} \to \{1, 2, 3, \ldots\}$. Sia $\mathcal{V} = \{u_1, \ldots, u_n\}$. La *realizzazione geometrica* di $K = (\mathcal{V}, \Sigma, \omega)$ è l'insieme Δ_K di tutti gli m-simplessi

$$T = \operatorname{conv}(e_{i(0)}/\omega(u_{i(0)}), \ldots, e_{i(m)}/\omega(u_{i(m)})) \subseteq \mathbb{R}^n, \quad (m = 0, \ldots, n)$$

tali che $\{u_{i(0)}, \ldots, u_{i(m)}\}$ appartiene a Σ. Dato un elemento $a \notin \mathcal{V}$ e un sottinsieme $A = \{a_1, \ldots, a_h\} \in \Sigma$, la *suddivisione semplice pesata* $(A, a)K$ è il complesso simpliciale astratto pesato in cui la suddivisione semplice $(A, a)(\mathcal{V}, \Sigma)$ viene dotata della funzione peso $\omega': \mathcal{V} \cup \{a\} \to \mathbb{N}$ data da $\omega' \supseteq \omega$ e $\omega'(a) = \omega(a_1) + \cdots + \omega(a_h)$. Due complessi simpliciali astratti pesati $K = (\mathcal{V}, \Sigma, \omega)$ e $K' = (\mathcal{V}', \Sigma', \omega')$ sono detti *equivalenti*, in simboli $K \sim K'$, se sono collegati da un cammino di suddivisioni semplici pesate e loro inverse. Un caso particolare di equivalenza si ha quando K è *combinatoriamente isomorfo* a K', in simboli, $K \cong K'$. Ciò significa che esiste una corrispondenza biunivoca β tra $\mathcal{V}$ e $\mathcal{V}'$ con queste due proprietà: per ogni $u \in \mathcal{V}$, $\omega'(\beta(u)) = \omega(u)$, e per ogni sottinsieme $\{a_1, \ldots, a_k\}$ di $\mathcal{V}$, $\{a_1, \ldots, a_k\} \in \Sigma \Leftrightarrow \{\beta(a_1), \ldots, \beta(a_k)\} \in \Sigma'$.

La seguente variante del Teorema 1.1 classifica i poliedri razionali a meno di $\mathbb{Z}$-omeomorfismo:

TEOREMA 2.1. – *La funzione $K \mapsto |\Delta_K|$ determina una corrispondenza biunivoca tra le classi di equivalenza dei complessi simpliciali astratti pesati e le classi di $\mathbb{Z}$-omeomorfismo dei poliedri razionali.*

Il terzo protagonista di queste pagine è la logica infinito-valente proposizionale $Ł_\infty$ di Łukasiewicz, [48]. Le formule di $Ł_\infty$ sono le stesse della logica booleana (con le variabili $v_1, v_2, \ldots$, la costante 1, la negazione $\neg$, e la congiunzione $\odot$). Gli assiomi di $Ł_\infty$, scritti in forma equazionale, sono

$$x \odot y = y \odot x, \quad x \odot (y \odot z) = (x \odot y) \odot z, \quad x \odot 1 = x \tag{1}$$

$$\neg\neg x = x, \quad x \odot \neg 1 = \neg 1, \quad y \odot \neg(y \odot \neg x) = x \odot \neg(x \odot \neg y). \tag{2}$$

Queste equazioni, dovute a Mangani che semplificò le equazioni originali di Chang, sono una riformulazione delle tautologie che Łukasiewicz congetturò (e

Chang stesso provò) essere sufficienti per ricavare tutte le tautologie della sua logica infinito-valente applicando le solite regole di sostituzione di eguali con eguali. Esse definiscono una classe di strutture, le MV-algebre, profondamente collegate con il resto della matematica [3], [8]-[11], [14],[19], [21], [25]-[37], [40]-[42], [45]. Aggiungendo l'equazione $x \odot x = x$ otteniamo la definizione di algebra di Boole.

Come le formule della logica booleana descrivono le funzioni booleane, così vedremo che le formule di $Ł_\infty$ descrivono le funzioni di McNaughton. Una *funzione di McNaughton* è una funzione continua $f\colon [0,1]^n \to [0,1]$ per cui esistono polinomi lineari (nel senso affine) $l_1, \ldots, l_k$ con coefficienti interi tali che per ogni $x \in [0,1]^n$ c'è un $i = 1, \ldots, k$ con $f(x) = l_i(x)$. Scriviamo $\mathcal{M}([0,1]^n)$ per la MV-algebra di tutte le funzioni di McNaughton definite sull'n-cubo $[0,1]^n$, con le operazioni $\neg f = 1 - f$ e $f \odot g = \max(0, f + g - 1)$. Più generalmente, per ogni sottinsieme chiuso e non vuoto X di $[0,1]^n$, denotiamo con $\mathcal{M}(X)$ la MV-algebra delle restrizioni a X delle funzioni di $\mathcal{M}([0,1]^n)$.

Come ogni classe definita da equazioni, anche le MV-algebre hanno oggetti liberi e presentazioni mediante un numero finito di generatori e relazioni, su cui ci soffermeremo più avanti:

TEOREMA 2.2. – *La funzione $P \mapsto \mathcal{M}(P)$ induce una corrispondenza biunivoca tra le classi di $\mathbb{Z}$-omeomorfismo dei poliedri razionali e le classi di isomorfismo delle MV-algebre finitamente presentate.*

Per non appesantire la lettura daremo solo i riferimenti e gli strumenti essenziali per ricostruire le dimostrazioni dei Teoremi 2.1 e 2.2. Per il trasferimento da una classe di oggetti all'altra useremo tecniche disparate, tra cui la procedura di desingolarizzazione delle varietà toriche (nella versione combinatoria nel linguaggio dei fan), la soluzione di Włodarczyk-Morelli della congettura debole di Oda sulla decomposizione di mappe toriche in blowup and blowdown, l'algoritmo di Hirzebruch-Jung a frazioni continue, e una variante del teorema del corpo convesso nella Geometria dei Numeri.

3. – Materiali per la dimostrazione del Teorema 2.1.

Come spesso succede in matematica, la dimostrazione richiede lo sviluppo di idee e nozioni che non appaiono esplicitate nell'enunciato principale.

3.1 – *Complesso, suddivisione, blowup*

Facciamo riferimento a [46, § 2] per tutte le nozioni di topologia poliedrale non definite in queste pagine. Salvo avviso contrario, ogni complesso ∇ sarà simpliciale, e quindi ometteremo l'aggettivo "simpliciale". Per ogni complesso ∇ l'unione punto a punto dei simplessi di ∇ si chiama il *supporto* di ∇ e si denota $|\nabla|$. Si dice anche che ∇ determina una *triangolazione* di $|\nabla|$. Dati due complessi ∇' e ∇ con lo stesso supporto diciamo che ∇' è una *suddivisione* di ∇ se ogni simplesso di ∇' è contenuto in qualche simplesso di ∇. Per ogni $c \in |\nabla| \subseteq \mathbb{R}^n$, il *blowup* $\nabla_{(c)}$ *di* ∇ *in* c è la suddivisione di ∇ ottenuta sostituendo ogni simplesso $C \in \nabla$ che contiene c con l'insieme di tutti i simplessi della forma $\mathrm{conv}(F \cup \{c\})$, ove F è un'arbitraria faccia di C che non contiene c. L'inversa di un blowup si chiama *blowdown* (si veda [52, p. 376] e [13, III, 2.1]).

3.2 – *Corrispondenti omogenei, fan.*

Per ogni punto razionale $y \in \mathbb{R}^n$ denotiamo con $\mathrm{den}(y)$ il minimo comune denominatore delle coordinate di y. Il vettore intero $\tilde{y} = \mathrm{den}(y)(y, 1) \in \mathbb{Z}^{n+1}$ si chiama il *corrispondente omogeneo* di y.

Per ogni m-simplesso razionale $T = \mathrm{conv}(w_0, \dots, w_m) \subseteq \mathbb{R}^n$ usiamo la notazione

$$T^{\uparrow} = \mathbb{R}_{\geq 0}\, \tilde{w}_0 + \cdots + \mathbb{R}_{\geq 0}\, \tilde{w}_m = \text{ cono in } \mathbb{R}^{n+1} \text{ generato da } \tilde{w}_0, \dots, \tilde{w}_m.$$

Diremo che il complesso ∇ è *razionale* se tutti i suoi simplessi sono razionali: in questo caso l'insieme $\nabla^{\uparrow} = \{T^{\uparrow} \mid T \in \nabla\}$ è noto come *fan simpliciale*, [13, 39].

3.3 – *Regolarità di un complesso e sua astrazione.*

Diciamo che il simplesso $T = \mathrm{conv}(w_0, \dots, w_m) \subseteq \mathbb{R}^n$ è *regolare* se è razionale e i corrispondenti omogenei $\{\tilde{w}_0, \dots, \tilde{w}_m\}$ dei suoi vertici sono parte di una base nel gruppo abeliano libero $\mathbb{Z}^{n+1}$. Un complesso razionale Δ è detto *regolare* se così è ogni suo simplesso. In altre parole, il fan $\Delta^{\uparrow}$ è regolare, [13, V, § 4] (= non singolare [39]). Un esempio di complesso regolare è dato dalla realizzazione geometrica Δ_K di ogni complesso simpliciale astratto pesato K. L'*astrazione* di un complesso regolare Δ è il complesso simpliciale astratto pesato $K_\Delta = (\mathcal{V}, \Sigma, \omega)$, ove (i) $\mathcal{V} =$ insieme dei vertici di Δ, (ii) per ogni sottinsieme $W = \{u_1, \dots, u_k\}$ di $\mathcal{V}$, $W \in \Sigma \Leftrightarrow \mathrm{conv}(u_1, \dots, u_k) \in \Delta$, e (iii) per ogni vertice w di Δ, $\omega(w) = \mathrm{den}(w)$.

3.4 – *Mediante di Farey.*

La *mediante di Farey* di un m-simplesso regolare $T = \mathrm{conv}(w_0, \dots, w_m) \subseteq \mathbb{R}^n$ è quel punto razionale w di T il cui corrispondente omogeneo $\tilde{w}$ coincide con $\tilde{w}_0 + \cdots + \tilde{w}_m$. Se T appartiene a un complesso regolare Δ e w è la mediante di Farey di T, allora il blowup $\Delta_{(w)}$ è ancora un complesso regolare.

Il primo pezzo della dimostrazione del Teorema 2.1 è il seguente “lemma di desingolarizzazione”, la cui idea centrale sarà usata ripetutamente nel seguito:

LEMMA 3.1. – *Un insieme non vuoto di* $[0,1]^n$ *è un poliedro razionale se e solo se coincide col supporto di un complesso regolare.*

DIMOSTRAZIONE (Cfr. [34, Proposition 1]). – Per la direzione non banale scriviamo $P = \bigcup T_i$ per opportuni simplessi razionali $T_1, \ldots, T_r$. La classica costruzione di una triangolazione di P, [46, 2.11], produce un complesso razionale Θ con supporto P. La procedura di desingolarizzazione descritta in [13, VI, 8.5] fornisce una suddivisione regolare Θ^* del fan simpliciale $\Theta^\uparrow = \{T^\uparrow \mid T \in \Theta\} \subseteq \mathbb{R}^{n+1}$. Intersecando ogni cono di Θ^* con l'iperpiano $x_{n+1} = 1$ abbiamo un complesso ∇ con supporto $P \times \{1\}$. Cancellando l'ultima coordinata dai vertici dei simplessi di ∇ otteniamo il desiderato complesso regolare con supporto P. □

Il secondo pezzo della dimostrazione del Teorema 2.1 è il seguente lemma, che richiede solo una diligente digestione di definizioni:

LEMMA 3.2. – *Siano* K *e* K' *complessi simpliciali astratti pesati. Siano* Δ *e* Δ' *complessi regolari con* $|\Delta| \subseteq \mathbb{R}^n$ *e* $|\Delta'| \subseteq \mathbb{R}^{n'}$. *Segue che*

1) $K \cong K_{\Delta_K}$.

2) *Sia* $\Delta_{(a)}$ *il blowup di* Δ *nella mediante di Farey* a *del simplesso*

$$T = \mathrm{conv}(w_1, \ldots, w_k) \in \Delta.$$

Allora $K_{\Delta_{(a)}} \cong (\{w_1, \ldots, w_k\}, a)K_\Delta$, *e quindi* $K_{\Delta_{(a)}} \sim K_\Delta$.

3) *Supponiamo che esista un isomorfismo combinatorio* $\theta: K_\Delta \cong K_{\Delta'}$. *Allora esiste uno* $\mathbb{Z}$*-omeomorfismo* η *di* $|\Delta|$ *su* $|\Delta'|$ *tale che* $\eta(w) = \theta(w)$ *per ogni vertice* w *di* Δ, *e* η *è lineare su ogni simplesso di* Δ.

4) $|\Delta| \cong_{\mathbb{Z}} |\Delta_{K_\Delta}|$.

5) *Per ogni poliedro razionale* $P \subseteq \mathbb{R}^m$ *esiste un complesso simpliciale astratto pesato* K *tale che* $|\Delta_K| \cong_{\mathbb{Z}} P$.

6) $K \sim K' \Rightarrow |\Delta_K| \cong_{\mathbb{Z}} |\Delta_{K'}|$.

La dimostrazione del Teorema 2.1 termina provando l'inversa dell'implicazione (6):

LEMMA 3.3. – $|\Delta_K| \cong_{\mathbb{Z}} |\Delta_{K'}| \Rightarrow K \sim K'$.

DIMOSTRAZIONE. – Per brevità scriviamo $P = |\Delta_K|$ e $P' = |\Delta_{K'}|$. Scriviamo anche $K = (\mathcal{V}, \Sigma, \omega)$ e $K' = (\mathcal{V}', \Sigma', \omega')$.

Sia dunque $\eta: P \cong_{\mathbb{Z}} P'$, e siano $\eta_1, \ldots, \eta_{n'}: P \to \mathbb{R}$ le sue componenti.

Prima Affermazione. Esiste un complesso regolare Λ con supporto $|\Delta_K|$ tale che η è lineare su ogni simplesso di Λ.

Sia $\mathcal{C}_0$ un complesso regolare con supporto P come dato dal Lemma 3.1. Per ogni $i = 1, \dots, n'$ siano $l_{i1}, \dots, l_{ik}$ i pezzi lineari della componente η_i. Facendo variare σ su tutte le permutazioni dell'insieme $\{1, \dots, k\}$, la collezione di insiemi $P_\sigma = \{x \in P \mid l_{i\sigma(1)} \leq \ldots \leq l_{i\sigma(k)}\}$ determina un complesso (razionale e poliedrale) $\mathcal{C}_i$ con supporto P, avente questa proprietà: le funzioni $l_{i1}, \dots, l_{ik}$ sono *stratificate* su ogni poliedro R di $\mathcal{C}_i$; in altre parole, per ogni $j' \neq j''$ abbiamo $l_{ij'} \leq l_{ij''}$ oppure $l_{ij'} \geq l_{ij''}$ su tutto R. Senza perdita di generalità ogni poliedro di $\mathcal{C}_i$ è un simplesso, ed inoltre $\mathcal{C}_i$ è una suddivisione di $\mathcal{C}_0$. Pertanto η_i è lineare su ogni simplesso di $\mathcal{C}_i$. Una costruzione di routine ci dà ora una suddivisione comune $\mathcal{C}$ di tutti i complessi razionali $\mathcal{C}_1, \dots, \mathcal{C}_{n'}$, tale che ogni simplesso di $\mathcal{C}$ è razionale. Evidentemente η è lineare su ogni simplesso di $\mathcal{C}$.

Desingolarizzando il fan simpliciale $\mathcal{C}^\uparrow = \{T^\uparrow \mid T \in \mathcal{C}\}$ come nella dimostrazione del Lemma 3.1 otteniamo un complesso regolare Λ con supporto P tale che η è lineare su ogni simplesso di Λ. La prima affermazione è dimostrata.

Denotiamo con $\Lambda' = \eta(\Lambda) = \{\eta(T) \mid T \in \Lambda\}$ il complesso simpliciale razionale immagine di Λ. Fissiamo un simplesso razionale $S = \mathrm{conv}(w_0, \dots, w_j) \subseteq P$ di Λ, con la sua immagine $S' = \eta(S)$. La funzione (affine) lineare $\eta\colon x \in S \mapsto y \in S'$ determina la funzione lineare omogenea $\eta_S^\uparrow\colon (x,1) \mapsto (y,1)$. Sia infatti M_S la matrice intera $(n'+1) \times (n+1)$ la cui ultima riga ha la forma $(0,0,\dots,0,0,1)$, con n zeri, e la cui i-ma riga ($i = 1, \dots, n'$) è data dai coefficienti di un polinomio lineare a coefficienti interi (scelto tra i pezzi lineari di η_i) che eguaglia la restrizione $\eta_i \restriction S$.

Allora $M_S(x,1) = (y,1) = \eta_S^\uparrow(x,1)$. Sia $S^\uparrow = \mathbb{R}_{\geq 0}\tilde{w}_0 + \cdots + \mathbb{R}_{\geq 0}\tilde{w}_j$ il cono generato dai corrispondenti omogenei dei vertici di S. Sia poi $S'^\uparrow$ il cono generato dai vettori interi $M_S\tilde{w}_0, \dots, M_S\tilde{w}_j$. Segue che M_S induce una corrispondenza biunivoca tra i punti interi di $S^\uparrow$ e i punti interi di $S'^\uparrow$. La nostra ipotesi su η, combinata con il teorema del corpo convesso nella Geometria dei Numeri (nel caso speciale del teorema di Blichfeldt [4, 17]) ci dice che S è regolare se e solo se il parallelepipedo semiaperto $Q_S = \{\mu_0\tilde{w}_0 + \cdots + \mu_j\tilde{w}_j \mid 0 \leq \mu_0, \dots, \mu_j < 1\}$ non contiene punti interi diversi dall'origine se e solo se lo stesso vale per la sua immagine $M_S(Q_S)$ se e solo se S' è regolare. Visto che S è regolare abbiamo dimostrato la seguente

Seconda Affermazione. Per ogni complesso regolare Λ tale che η sia lineare su ogni simplesso di Λ, il complesso $\Lambda' = \eta(\Lambda)$ è regolare con supporto P'.

Osservando che per ogni punto razionale $z \in P$, $\mathrm{den}(\eta(z)) = \mathrm{den}(z)$, otteniamo ora un isomorfismo combinatorio $K_\Lambda \cong K_{\Lambda'}$.

Per concludere, siccome Δ' e $\Delta_{K'}$ sono complessi regolari con lo stesso supporto P', esiste un cammino di blowup e blowdown che trasforma Δ' in $\Delta_{K'}$. Analogamente esiste un cammino di blowup e blowdown che trasforma Δ in Δ_K. Ciò è conseguenza della (versione affine della) soluzione della congettura debole di Oda, ad opera di Włodarczyk e Morelli, [52, 13.3], [23]. Ricordando il Lemma 3.2 possiamo scrivere $K \cong K_{\Delta_K} \sim K_\Delta \cong K_{\Delta'} \sim K_{\Delta_{K'}} \cong K'$. Siccome ogni isomorfismo combinatorio è ottenibile con un numero finito di suddivisioni semplici pesate, concludiamo che $K \sim K'$, il che completa la dimostrazione del lemma. □

La dimostrazione del Teorema 2.1 è così terminata.

COROLLARIO 3.4. – *L'inversa della corrispondenza determinata dalla funzione $K \mapsto |\Delta_K|$ del Teorema 2.1 è la corrispondenza determinata dalla funzione che porta il supporto $|\Delta|$ di ogni complesso regolare nel complesso simpliciale astratto pesato K_Δ astrazione di Δ.*

Dunque

$$\boxed{\mathbb{Z}\text{-omeomorfismo} = \text{collegamento con un cammino di blowup e blowdown}}$$

3.5 – *Digressione: $\mathbb{Z}$-omeomorfismo ed equidissezionabilità*

Seguendo [22, 1.4], per *dissezione* di un poliedro razionale $P \subseteq \mathbb{R}^d$ intendiamo un'espressione della forma $P = P_1 \dot\cup \cdots \dot\cup P_k$ per opportuni poliedri razionali $P_1, \ldots, P_k \subseteq \mathbb{R}^d$. Questa è una notazione abbreviata per dire che $P = P_1 \cup \cdots \cup P_k$ e l'interno di $P_i \cap P_j$ è vuoto per ogni $i \neq j$. Sia G un gruppo di affinità di $\mathbb{R}^d$ che permuta l'insieme dei poliedri razionali contenuti in $\mathbb{R}^d$. Due poliedri razionali $P, Q \subseteq \mathbb{R}^d$ sono detti *G-equidissezionabili* se esistono dissezioni $P = P_1 \dot\cup \cdots \dot\cup P_k$ e $Q = Q_1 \dot\cup \cdots \dot\cup Q_k$, ed elementi $\varphi_1, \ldots, \varphi_k \in G$ tali che $Q_i = \varphi_i(P_i)$ ogni $i = 1, \ldots, k$. Se inoltre per ogni i, j con $1 \leq i < j \leq k$, φ_i coincide con φ_j su $P_i \cap P_j$, e φ_i^{-1} coincide con φ_j^{-1} su $Q_i \cap Q_j$, allora diciamo che P e Q sono G-equidissezionabili *con continuità*. Denotiamo con $\mathcal{G} = GL(d, \mathbb{Z}) \ltimes \mathbb{Z}^d$ il gruppo delle *trasformazioni unimodulari*, ossia quelle affinità di $\mathbb{R}^d$ che conservano il reticolo $\mathbb{Z}^d$, [12, 1.3], [22, 5.6]. Vale questo risultato, la cui dimostrazione apparirà altrove:

TEOREMA 3.5. – *Due polinomi razionali P e Q in $\mathbb{R}^d$ sono $\mathbb{Z}$-omeomorfi se e solo se sono $\mathcal{G}$-equidissezionabili con continuità.*

Dunque

$$\boxed{\mathbb{Z}\text{-omeomorfismo} = \mathcal{G}\text{-equidissezione continua, per } \mathcal{G} = GL(d, \mathbb{Z}) \ltimes \mathbb{Z}^d}$$

4. – Materiali per la dimostrazione del Teorema 2.2.

Introduciamo in questa sezione alcuni strumenti necessari per la dimostrazione del Teorema 2.2, e di per sé interessanti, vista la ricchezza delle MV-algebre. Per tutto quanto non spiegato qui facciamo riferimento alla monografia [9].

I *termini* del linguaggio delle MV-algebre sono costruiti partendo dalle variabili v_i e applicando i simboli di $1, \neg, \odot$ come nel caso booleano. Fissiamo $n = 1, 2, \ldots$. Per ogni $i = 1, \ldots, n$, scriviamo $\pi_i \colon [0,1]^n \to [0,1]$ per denotare la i-ma funzione identità, $\pi_i(x_1, \ldots, x_n) = x_i$. Per induzione definiamo ora la funzione $\mathbf{f} \colon \{\text{termini}\} \to \mathcal{M}([0,1]^n)$ come segue:

$$v_i \mapsto \mathbf{f}_{v_i} = \pi_i, \quad \neg\,\tau \mapsto \neg\,\mathbf{f}_\tau = 1 - \mathbf{f}_\tau, \quad \tau \odot \sigma \mapsto \mathbf{f}_\tau \odot \mathbf{f}_\sigma = \max(0, \mathbf{f}_\tau + \mathbf{f}_\sigma - 1). \tag{3}$$

Due MV-termini σ e τ nelle variabili $v_1, \ldots, v_n$ sono (logicamente) *equivalenti* se $\mathbf{f}_\tau = \mathbf{f}_\sigma$. Denotiamo con $|\tau|$ la classe di equivalenza di τ (2). Come dimostrato in [9, 3.1.4, 4.5.5] le classi di equivalenza dei termini formano la *MV-algebra libera* $Free_n$ sui generatori $|v_1|, \ldots, |v_n|$. Dalla proprietà universale di $Free_n$ segue che la funzione $|v_i| \mapsto \pi_i$ si estende canonicamente ad un omomorfismo $\imath$ di $Free_n$ in $\mathcal{M}([0,1]^n)$.

Il teorema di completezza di Chang [9, 2.5.3, 4.5.2] e il teorema di McNaughton [9, 9.1.5] assicurano rispettivamente che $\imath$ è iniettivo e suriettivo,

$$\imath \colon Free_n \cong \mathcal{M}([0,1]^n). \tag{4}$$

Un *ideale* di una MV-algebra A è il kernel J di un omomorfismo di A. Diciamo che J è *principale* se esiste un elemento $a \in A$ tale che J è l'intersezione di tutti gli ideali che contengono a.

Una MV-algebra è *finitamente presentata* se è il quoziente di una MV-algebra libera $Free_n$ per un suo ideale principale.

Combinando [21, 5.2], con l'equivalenza categoriale [25, 3.9] si ottiene questa generalizzazione della rappresentazione (4):

TEOREMA 4.1. – *Una MV-algebra è finitamente presentata se e solo se è isomorfa a una MV-algebra $\mathcal{M}(P)$ per qualche poliedro razionale P.*

Utilizzando questo teorema si ottiene il Teorema 2.2. Per brevità risparmiamo al lettore i dettagli finali della dimostrazione, che appariranno altrove. Facciamo solo due osservazioni: (i) Ogni poliedro razionale Q in $\mathbb{R}^n$ possiede una copia $\cong_{\mathbb{Z}}$-omeomorfa P contenuta in qualche m-cubo, per m abbastanza grande (Lemma 3.2(v)).

(2) Per i lettori interessati a questioni di complessità algoritmica, notiamo che il problema di decidere se due termini sono equivalenti ha la stessa complessità del problema corrispondente per le formule booleane, ossia è co-NP-completo, [26], [9, 9.3].

(ii) I poliedri razionali sono precisamente gli zeroset $f^{-1}(0)$ delle funzioni di McNaughton (Lemma 3.1 insieme con [21, 5.1]).

Componendo i Teoremi 2.2 e 2.1 otteniamo:

COROLLARIO 4.2. – *La funzione $K \mapsto \mathcal{M}(|\Delta_K|)$ determina una corrispondenza biunivoca tra le classi di equivalenza dei complessi simpliciali astratti pesati, e le classi di isomorfismo delle MV-algebre finitamente presentate.*

Nella Tabella 1 viene dato qualche esempio di questa corrispondenza.

Pertanto la nozione di $\mathbb{Z}$-omeomorfismo ha anche una controparte algebrica:

$$\boxed{\mathbb{Z}\text{-omeomorfismo} = \text{isomorfismo delle MV-algebre finitamente presentate}}$$

Tabella 1: Alcuni casi particolari del Corollario 4.2

Complesso simpliciale astratto pesato $(\mathcal{V}, \Sigma, \omega)$	MV-algebra finitamente presentata
$\mathcal{V} = \{u\}$ singoletto	sottalgebra finita di $[0,1] \cap \mathbb{Q}$
$\mathcal{V} = \{u\}$, $\omega(u) = l$	catena di Łukasiewicz $\{0, 1/l, \ldots, (l-1)/l, 1\}$
0-dimensionale (Σ non ha insiemi con 2 elementi)	prodotto finito di catene di Łukasiewicz
0-dimensionale, e $\omega(u) = l$ per ogni $u \in \mathcal{V}$	prodotto finito di catene a $(l+1)$ elementi
0-dimensionale, $\mathcal{V}$ ha 2^n elementi, $\omega = 1$	algebra booleana libera con n-generatori
$\Sigma = \{\emptyset, \{0\}, \{1\}, \{2\}\}$, $\omega(0) = \omega(1) = 1, \omega(2) = 2$	MV_3-algebra libera su 1 generatore, [9, 8.5]
$\{\emptyset, \{0\}, \{1\}, \{0,1\}\}$, $\omega(0) = \omega(1) = 1$	MV-algebra libera su 1 generatore $\mathcal{M}([0,1])$
$K_{\mathcal{K}^*}$, ($\mathcal{K}^*$ = triangolazione standard [47] di $[0,1]^n$)	MV-algebra libera su n generatori $\mathcal{M}([0,1]^n)$
ogni insieme di Σ ha $\leq n$ elementi	$\mathcal{M}(P)$, $\dim(P) < n$, P poliedro razionale
Σ = tutti i sottinsiemi di $\{1, \ldots, n\}$, $\omega = 1$	$\mathcal{M}(\{(x_1, \ldots, x_n) \in [0,1]^n \mid \sum x_i = 1\})$
$\{\emptyset, \{0\}, \{u\}, \{0,u\}\}$, $\omega(0) = 1$, $\omega(u) = d$	$\mathcal{M}([0, 1/d])$

5. – Applicazioni: invarianti, misure, algoritmi.

5.1 – *Variazioni sul terzo problema di Hilbert.*

Con riferimento ai problemi posti dal Teorema 1.2, in questa sezione daremo una lista—non completa, ma abbastanza ricca di informazione—di invarianti per lo $\mathbb{Z}$-omeomorfismo dei poliedri razionali, assieme a una procedura per calcolare effettivamente tali invarianti. Alla luce del Teorema 3.5 essi sono anche utili strumenti per quella variante del terzo problema di Hilbert che chiede condizioni necessarie e sufficienti per la $\mathcal{G}$-equidissezionabilità di due poliedri (razionali) in termini di famiglie di invarianti (effettivamente calcolabili) ([3]).

([3]) Come noto, il problema nella sua formulazione originale fu risolto immediatamente.

Sia $P \subseteq \mathbb{R}^n$ un poliedro razionale e Δ un complesso regolare con supporto P. Denotiamo con $\Delta^{\max}(d)$ l'insieme dei d-simplessi massimali di Δ, ossia quelli che non sono contenuti propriamente in nessun simplesso di Δ.

Per ogni d-simplesso regolare $R = \mathrm{conv}(w_0, \ldots, w_d) \subseteq \mathbb{R}^n$ denotiamo con $\mathrm{den}(R)$ il prodotto $\mathrm{den}(w_0) \cdots \mathrm{den}(w_d)$, ove $\mathrm{den}(x)$ è come in 3.2.

TEOREMA 5.1. – *Per ogni $i = 0, 1, \ldots,$ poliedro razionale $P \subseteq \mathbb{R}^n$, e complesso regolare Δ con supporto P poniamo $\lambda_i(P, \Delta) = \sum \left\{(i!\ \mathrm{den}(S))^{-1} \mid S \in \Delta^{\max}(i)\right\}$, ove la somma vale zero se $\Delta^{\max}(i)$ è vuoto. Allora abbiamo:*

(i) *Per ogni complesso regolare ∇ con supporto P vale l'identità $\lambda_i(P, \Delta) = \lambda_i(P, \nabla)$, e possiamo scrivere senza ambiguità $\lambda_i(P) = \lambda_i(P, \Delta) = \lambda_i(P, \nabla)$.*

(ii) *La quantità $\lambda_n(P)$ coincide con la misura di Lebesgue n-dimensionale $\lambda(P)$. Inoltre per ogni $m < n$, se il poliedro $\bigcup\{Q \mid Q \in \Delta^{\max}(m)\} \subseteq P$ ha una copia $\mathbb{Z}$-omeomorfa R contenuta in $\mathbb{R}^m$ allora $\lambda_m(P)$ coincide con la misura di Lebesgue m-dimensionale di R.*

(iii) *Se $P' \subseteq \mathbb{R}^{n'}$ è un poliedro razionale e $P \cong_{\mathbb{Z}} P'$ allora $\lambda_j(P) = \lambda_j(P')$ per ogni $j = 0, 1, 2, \ldots$.*

(iv) *La funzione $P \mapsto (\lambda_0(P), \ldots, \lambda_n(P))$ è effettivamente calcolabile.*

DIMOSTRAZIONE. – Le affermazioni (i) e (ii) sono dimostrate in [34, 2.1]. Per una dimostrazione della proprietà di invarianza (iii) si veda [34, 4.1, Claim 2]. Per dimostrare (iv) non importa se la presentazione di $P = \bigcup_1^t T_i$ consiste nell'elenco dei vertici di ogni simplesso T_i, oppure T_i è presentato come intersezione di un numero finito di semispazi chiusi $H_{y,z} = z + \{x \in \mathbb{R}^n \mid x \circ y \geq 0\}$, ove y e z sono vettori razionali in $\mathbb{R}^n$ e $\circ$ denota il prodotto scalare: infatti il primo tipo di presentazione è effettivamente trasformabile nel secondo, e viceversa, [51]. La dimostrazione di [46, 2.11] contiene una procedura effettiva per costruire un complesso (simpliciale e razionale) Θ con supporto P. La procedura di desingolarizzazione descritta in [13, VI, 8.5] computa in maniera effettiva una suddivisione regolare $\Theta^\sharp$ del fan simpliciale $\Theta^\uparrow = \{T^\uparrow \mid T \in \Theta\}$: ogni passo della procedura consiste nella ricerca di un punto intero nonzero w in un poliedro convesso razionale esplicitamente dato, e nella costruzione del blowup in w di un fan esplicitamente dato. Partendo da $\Theta^\sharp$ e seguendo i passi finali della dimostrazione del Lemma 3.1, che sono tutti effettivi, otteniamo un complesso regolare Δ con supporto P. Si può ora calcolare ogni razionale $\lambda_i(P, \Delta)$, che per (i) coincide con $\lambda_i(P)$. □

Nonostante la stretta analogia tra complessi e fan, il teorema appena dimostrato non ha analoghi per i fan regolari.

5.2 – *Metamorfosi di problemi di decisione.*

Una lettura anche solo in filigrana di tutte le costruzioni e le affermazioni esistenziali delle pagine precedenti mostra la loro natura effettiva. Ciò vale in particolare per la procedura di desingolarizzazione usata nel Lemma 3.1, che costruisce un complesso regolare su ogni poliedro razionale P. La funzione $K \mapsto |\Delta_K|$ del Teorema 2.1 è effettivamente calcolabile, e così è pure l'astrazione K_Δ di ogni complesso regolare Δ.

Per quanto riguarda la funzione $P \mapsto \mathcal{M}(P)$ del Teorema 2.2 e la sua inversa, occorre chiarire che cosa si intende per una "presentazione finita" di una MV-algebra. La definizione è la stessa che per i gruppi, o per qualsiasi struttura in una classe equazionale. Attraverso la definizione induttiva (3), ogni termine $\tau(v_1, \ldots, v_n)$ nel linguaggio delle MV-algebre rappresenta la funzione di McNaughton $\mathbf{f}_\tau$, che alla luce dell'isomorfismo (4) è un elemento della MV-algebra libera $\mathcal{M}([0,1]^n)$ su n generatori; la funzione $\mathbf{f}_\tau$ genera un ideale (ipso facto principale) J_τ di $\mathcal{M}([0,1]^n)$, e si dice che τ è una *presentazione finita* della MV-algebra quoziente $A_\tau = \mathcal{M}([0,1]^n)/J_\tau$. Questa terminologia è giustificata dal fatto che τ è una stringa finita di simboli di un alfabeto precostituito; variando τ su tutti i termini MV-algebrici si ottiene ogni possibile presentazione finita [4].

Il carattere effettivo delle corrispondenze dei Teoremi 2.1 e 2.2 garantisce la validità del seguente

COROLLARIO 5.2. – *Consideriamo questi problemi:*

(i) *Se due complessi simpliciali astratti pesati siano equivalenti.*
(ii) *Se due poliedri razionali siano $\mathbb{Z}$-omeomorfi.*
(iii) *Se due MV-algebre finitamente presentate siano isomorfe.*

Allora la (in)decidibilità di uno qualsiasi di questi problemi implica la (in)decidibilità degli altri due.

Nonostante il risultato di indecidibilità di Markov citato nell'introduzione, non vi è nella letteratura una dimostrazione di indecidibilità per il problema proteiforme (i)-(iii).

Un risultato molto speciale di riconoscibilità è il seguente:

TEOREMA 5.3. – *È decidibile il problema se un poliedro razionale $P \subseteq \mathbb{R}^n$, $n = 1, 2, \ldots$, sia o no $\mathbb{Z}$-omeomorfo all'intervallo reale* $[0,1]$.

Dunque è decidibile se una MV-algebra finitamente presentata sia o no isomorfa alla MV-algebra libera su un generatore. La dimostrazione, che apparirà

[4] Come $Free_n \cong \mathcal{M}([0,1]^n)$ è la MV-algebra delle classi di equivalenza di formule $\sigma(v_1, \ldots, v_n)$ della logica Ł_∞, così la MV-algebra A_τ è, a meno di isomorfismo, l'algebra delle classi di equivalenza di formule nella teoria $\Theta = \{\tau\}^\vdash$ data dalle conseguenze di τ, [9, 4.6.8]: σ' è detta essere *equivalente* a σ'' se la bi-implicazione $\sigma' \leftrightarrow \sigma''$ è conseguenza di τ.

altrove, con una banale ispezione preliminare decide se P è monodimensionale. In tal caso, P viene opportunamente dissezionato in intervalli regolari, utilizzando l'algoritmo di Hirzebruch-Jung a frazioni continue [15, 16]. Questa dissezione (minima) fornisce invarianti effettivamente calcolabili e *completi* per lo $\cong_{\mathbb{Z}}$-omeomorfismo. Il risultato è degno di nota perché mostra come la riconoscibilità dei poliedri sia intimamente connessa con la calcolabilità effettiva di invarianti completi.

Alla luce del risultato di A.A. Markov citato nell'introduzione e degli sviluppi successivi ad opera di S. P. Novikov sull'irriconoscibilità delle copie PL-omeomorfe dei simplessi, [5], è già interessante chiedersi se esistano invarianti completi e calcolabili che rendano riconoscibili le immagini $\mathbb{Z}$-omeomorfe del quadrato $[0,1]^2$, tra tutti i poliedri razionali.

5.3 – *Il teorema di Haar MV-algebrico*

Sia $P \subseteq \mathbb{R}^n$ un poliedro razionale, f una funzione di $\mathcal{M}(P)$ e Δ_f un complesso regolare su P tale che f è lineare su ogni simplesso di Δ_f. Tale Δ_f esiste per una variante dell'argomento di desingolarizzazione nel Lemma 3.1. Integriamo f su P con gli elementi di volume dx di ogni simplesso T di Δ_f misurati secondo il Teorema 5.1. Allora la funzione

$$s{:}\, f \mapsto \int_P f(x)\mathrm{d}x$$

opportunamente normalizzata costituisce uno *stato* di $\mathcal{M}(P)$, ossia una funzione $s{:}\,\mathcal{M}(P) \to \mathbb{R}$ tale che $s(1) = 1$ e $s(x \oplus y) = s(x) + s(y)$ quando $x \odot y = 0$. Come al solito la disgiunzione è definita da $x \oplus y = \neg(\neg x \odot \neg y)$. L'invarianza di s segue dall'invarianza di ciascun λ_d. Dalla soluzione della congettura debole di Oda segue che il valore $s(f)$ non dipende da Δ_f.

Inoltre s è *fedele*, nel senso che $s(f) = 0 \Leftrightarrow f = 0$.

Combinando [34, 4.1] con l'equivalenza categoriale di [25, 3.9] e con il Teorema 4.1 otteniamo così il seguente teorema di Haar MV-algebrico:

TEOREMA 5.4. – *Ogni MV-algebra finitamente presentata possiede uno stato fedele ed invariante per automorfismi.*

Gli stati sulle MV-algebre hanno importanza fondamentale per una teoria non booleana della probabilità algebrica alla maniera di Carathéodory, [45]. Nei suoi lavori [40]-[42] Panti ha esteso la teoria ergodica alle MV-algebre libere $Free_n$, dando una reinterpretazione MV-algebrica del differenziale di Tsujii [49], e una tersa caratterizzazione dell'integrale di Lebesgue, tra tutti gli stati invarianti di $Free_n$.

6. – MV-algebre e logica di Łukasiewicz

6.1 – *Mostowski, Rényi, Ulam*

In questa parte finale, più ricreativa, vedremo che le MV-algebre sono le algebre della logica proposizionale infinito-valente di Łukasiewicz, $Ł_\infty$. Vedremo anche che $Ł_\infty$ parla e ragiona con la stessa naturalezza del suo frammento bivalente dato dalla logica booleana. Il lettore avrà così elementi per valutare quanto è cambiata la nostra comprensione di $Ł_\infty$ dal tempo in cui Mostowski scrisse queste righe nella sua commemorazione di Łukasiewicz, [24, p. 5]:

> A l'heure actuelle il n'est pas possible d'émettre une opinion définitive se les logiques multivalentes ne resteront qu'une construction théorique philosophique ou si elles trouveront des applications en dehors de la logique la plus abstraite.

Il nostro punto di partenza è una variante del gioco "Pensa un Numero" (Twenty Questions) in cui parte delle risposte sono false/erronee. Il gioco è descritto da Rényi [44, page 47] come un problema di ricerca adattiva e fault-tolerant:

> Assume that the number of questions which can be asked to figure out the "something" being thought of is fixed and the one who answers is allowed to lie a certain number of times. The questioner, of course, doesn't know which answer is true and which is not. Moreover the one answering is not required to lie as many times as is allowed. For example, when only two things can be thought of and only one lie is allowed, then 3 questions are needed. [...] If there are four things to choose from and one lie is allowed, then five questions are needed. If two or more lies are allowed, then the calculation of the minimum number of questions is quite complicated. And I think that the game "with lies", when more than one lie is allowed, becomes too complicated for a game as such, but is pretty good at helping one to understand the difficulties encountered in the transmission of information via a noisy channel. It does seem to be a very profound problem: I am very curious to hear the proofs of the coding theorems.

Lo stesso gioco, e relativo problema, è descritto da Ulam [50, p. 281]:

> Someone thinks of a number between one and one million (which is just less than 2^{20}). Another person is allowed to ask up to twenty questions, to each of which the first person is supposed to answer only yes or no. Obviously the number can be guessed by asking first: Is the number in the first half million? then again reduce the reservoir of numbers in the next question by one-half, and so on. Finally the number is obtained in less than $\log_2(1000000)$. Now suppose one were allowed to lie once or twice, then how many questions would one need to get the right answer?

Per fissare le idee chiamiamo Pinocchio colui che risponde, e chiamiamo Ispettore colei/colui che fa domande. Dal punto di vista dell'Ispettore poco importa che le risposte siano errate perché Pinocchio è bugiardo, o perché non sa come rispondere, o perché la distorsione si incarica di corrompere fino a e tra i bit delle sue risposte sincere e accurate. Come nota Rényi, il gioco di Ulam–Rényi in realtà è un capitolo della teoria della trasmissione dell'informazione in un canale rumoroso con feedback, [2]. I lettori interessati ai problemi di ottimizzazione posti da Rényi e Ulam possono consultare, ad esempio, i lavori [6, 7, 43] e le loro estese bibliografie che coprono un vasto capitolo di matematica applicata. Basti dire che nel caso particolare, non adattivo, in cui tutte le domande sono poste in un unico questionario all'inizio del gioco, le strategie di ricerca sono note come codici e-correttori.

Essendo il nostro scopo quello di mostrare che i progressivi "stati di conoscenza" dell'Ispettore sono governati dalla logica a più valori di Łukasiewicz, guardiamo da vicino una partita: i giocatori fissano un insieme $\mathcal{S}$ di numeri, chiamato lo *spazio di ricerca*, e un intero $e \geq 0$. Pinocchio sceglie un numero $x_{segreto} \in \mathcal{S}$ che l'Ispettore deve trovare, facendo domande binarie. Nelle sue risposte sì-no Pinocchio può mentire fino a e volte. Per definizione, una *domanda* è un sottinsieme di $\mathcal{S}$: ad esempio la domanda "$x_{segreto}$ è dispari ?" è l'insieme dei numeri dispari di $\mathcal{S}$. Una *risposta* a questa domanda è un bit $b \in \{0,1\} = \{\text{no, si}\}$. Identificandoci con l'Ispettore, il nostro stato di conoscenza di $x_{segreto}$ durante la partita è unicamente determinato dalla sequenza di domande/risposte finora ricevute. (Ovviamente nel gioco di Rényi-Ulam il naso di Pinocchio non si allunga quando mente.)

Quando non vi sono bugie un resoconto completo del nostro stato di conoscenza a un certo istante è fornito dall'*insieme* R di tali coppie domande/risposte: infatti due risposte eguali alla stessa domanda ripetuta due volte contengono la stessa informazione di una sola risposta.

Per una ricerca intelligente di $x_{segreto}$ ci interessa riconoscere quando due insiemi R e Q sono equivalenti, ossia contengono esattamente la stessa informazione su $x_{segreto}$. Per ogni insieme R incarichiamo dunque la funzione $R^{\#}: \mathcal{S} \to \{0,1\}$ di dirci il *valore di verità* di ogni $z \in \mathcal{S}$, secondo R. Per definizione, il valore di verità di z è la quantità

$$(5) \qquad 1 \dot{-} \text{numero di risposte in } R \text{ falsificate da } z,$$

dove $\dot{-}$ denota la sottrazione troncata a zero. In altre parole, per ogni $z \in \mathcal{S}$, $R^{\#}(z)$ vale 1 se z soddisfa tutte le risposte di R, mentre $R^{\#}(z) = 0$ se z falsifica anche una sola risposta. Vediamo subito che due insiemi R e Q sono equivalenti se e solo se $R^{\#} = Q^{\#}$. Dunque le classi di equivalenza sono identificabili con le funzioni booleane su $\mathcal{S}$.

Passando al caso generale con e bugie, tutto quello che sappiamo su $x_{segreto}$ è ancora dato dal resoconto verbale R delle domande/risposte ricevute.

Tuttavia, ora R ha la struttura di *multinsieme*—perché risposte eguali alla stessa domanda ripetuta due volte contengono più informazione che una singola risposta ([5]). Dunque, ogni elemento di R ha una molteplicità, con cui teniamo conto di quante volte abbiamo ricevuto la stessa risposta. Generalizzando la definizione (5), ad ogni multinsieme R associamo la funzione $R^{\#}\colon \mathcal{S} \to \{0, 1/(e+1), 2/(e+1), \ldots, e/(e+1), 1\}$ definita da

$$R^{\#}(z) \;=\; 1 \dot{-} \frac{\text{numero di risposte in R falsificate da } z}{e+1}. \tag{6}$$

Detto altrimenti, per ogni $z \in \mathcal{S}$ il *valore di verità* $R^{\#}(z)$ di z è la distanza (misurata in unità di $e+1$) dalla condizione in cui z è eliminato dall'insieme dei possibili candidati per $x_{segreto}$. Diremo poi che due multinsiemi R e Q sono *equivalenti* se vale l'eguaglianza $R^{\#}(x) = Q^{\#}(x)$ per ogni $x \in \mathcal{S}$. La classe di equivalenza del multinsieme R è denotata $[R]$, oppure r se non vi è pericolo di confusione.

Uno *stato (di conoscenza)* nel gioco di Rényi-Ulam sullo spazio di ricerca $\mathcal{S}$ con e bugie è una classe di equivalenza $[R]$ di multinsiemi di domande/risposte. $[R]$ è *identificabile* con la funzione $R^{\#}\colon \mathcal{S} \to \{0, 1/(e+1), 2/(e+1), \ldots, e/(e+1), 1\}$. Lo stato *iniziale* 1 è la classe di equivalenza del multinsieme vuoto di chi non ha ancora ricevuto risposte: per la nostra identificazione, lo stato iniziale è la funzione costantemente eguale a 1 su $\mathcal{S}$. Lo stato *incompatibile* 0 è la classe di equivalenza di un multinsieme che non lascia più in gioco nessun candidato per $x_{segreto}$, ad esempio il multinsieme in cui l'insieme vuoto ha molteplicità $e+1$; esso descrive il nostro stato di conoscenza al termine di una partita in cui alla domanda " $x_{segreto}$ appartiene a $\mathcal{S}$?" ripetuta $e+1$ volte, Pinocchio ha sempre ostinatamente risposto no. (I veri bugiardi invece stanno ben attenti a non mentire troppo, sapendo che le bugie hanno le gambe corte). Per la nostra identificazione, lo stato incompatibile è la funzione costantemente eguale a 0 su $\mathcal{S}$.

L'insieme $\Sigma_{\mathcal{S},e}$ degli stati nel gioco di Rényi-Ulam su $\mathcal{S}$ con e bugie possiede la struttura di ordine parziale di ogni insieme di funzioni a valori reali: e noi diremo che uno stato $[R]$ è *più restrittivo di* $[Q]$, in simboli, $[R] \preceq [Q]$, se $R^{\#} \leq Q^{\#}$. Definendo poi l'*unione* di due multinsiemi $M \smile N$ come il multinsieme che dà a ciascuna risposta la somma delle molteplicità che essa ha in M e in N, vediamo che l'operazione $\smile$ induce su $\Sigma_{\mathcal{S},e}$ l'operazione $[M] \odot [N] = [M \smile N]$. L'operazione $\odot$ è commutativa, associativa, ed ha lo stato 1 come elemento neutro. Tra tutti gli stati di $\Sigma_{\mathcal{S},e}$ che sono incompatibili con un dato

([5]) Ad esempio, con $e = 1$ supponiamo di chiedere due volte "il numero è pari ?" . Se Pinocchio risponde sì a entrambe le domande, allora $x_{segreto}$ è davvero pari. Invece dopo una sola risposta non siamo sicuri che $x_{segreto}$ sia pari. Questa banale osservazione mostra che la logica del gioco con bugie non soddisfa il principio di idempotenza della logica classica.

stato r ne esiste uno minimamente restrittivo, che denotiamo $\neg r$; in altre parole, $r \odot \neg r = 0$, e se uno stato t soddisfa $t \odot r = 0$ segue che $t \leq \neg r$. L'operazione $\neg$ regala al monoide abeliano $\Sigma_{\mathcal{S},e}$ un'involuzione $r = \neg\neg r$ con la proprietà che $\neg 1 = 0, r \odot 0 = 0$ e $\neg(\neg r \odot q) \odot q = \neg(\neg q \odot r) \odot r$. Dando a $\Sigma_{\mathcal{S},e}$ le operazioni $\odot$ e $\neg$, con la costante $1 = \neg 0$, l'ordine diviene un sottoprodotto della struttura algebrica, essendo definibile da $r \preceq p \Leftrightarrow r \odot \neg p = 0$.

In definitiva, tutte le strutture $\langle \Sigma_{\mathcal{S},e}, \odot, \neg, 1\rangle$ sono MV-algebre. Il loro ruolo speciale è dato da questo teorema:

TEOREMA 6.1. – *Siano $\sigma = \sigma(v_1, \ldots, v_n)$ e $\tau = \tau(v_1, \ldots, v_n)$ termini nel linguaggio MV-algebrico. Allora le seguenti condizioni sono equivalenti per l'equazione $\sigma = \tau$:*

(i) *L'equazione è valida in ogni MV-algebra $\Sigma_{\mathcal{S},e}$.*
(ii) *L'equazione è valida in ogni MV-algebra.*
(iii) *La formula $\sigma \leftrightarrow \tau$ è una tautologia nella logica proposizionale infinito-valente $Ł_\infty$ di Łukasiewicz.*

DIMOSTRAZIONE. – L'equivalenza tra (ii) e (iii) è l'essenza logica del teorema di completezza di Chang [9, 2.5.3, 4.5.2]. Ci rimane da dimostrare l'implicazione (i) $\rightarrow$ (ii). Per ipotesi, l'equazione $\sigma = \tau$ è valida in tutte le MV-algebre $\Sigma_{\mathcal{S},e}$ in cui $\mathcal{S} = \{a\}$ è un singoletto. A meno di isomorfismo, $\Sigma_{\{a\},e}$ è la MV-algebra definita sull'insieme dei valori di verità $\{0, 1/(e+1), \ldots, e/(e+1), 1\}$, con le operazioni di negazione $x \mapsto \neg x = 1 - x$ e di congiunzione $(x, y) \mapsto x \odot y = \max(0, x + y - 1)$. Tale struttura è nota col nome di *catena di Łukasiewicz con $e+1$ elementi.* Vogliamo dimostrare che l'equazione vale in ogni MV-algebra. Procediamo per assurdo e supponiamo che l'equazione fallisca in una MV-algebra. Per il teorema di completezza di Chang l'equazione $\sigma = \tau$ fallisce anche nella MV-algebra $[0, 1]$ (con le operazioni di negazione e congiunzione definite precedentemente). Siccome tali operazioni sono continue e trasformano razionali in razionali, l'equazione $\sigma = \tau$ fallisce nella sottalgebra $[0, 1] \cap \mathbb{Q}$. Dunque esistono numeri razionali $c_1, \ldots, c_n$ tali che $\sigma(c_1, \ldots, c_n) \neq \tau(c_1, \ldots, c_n)$. I sottotermini di σ e τ individuano un insieme finito I di razionali, diciamo $I = \{c_1, \ldots, c_n, c_{n+1}, \ldots, c_u\}$. Detto d il minimo comune multiplo dei numeri in I, concludiamo che l'equazione fallisce nella catena di Łukasiewicz con $d+1$ elementi $\{0, 1/d, \ldots, (d-1)/d, 1\}$, contraddizione. □

Questo teorema ci dice che le formule $\sigma \leftrightarrow \tau$ valide nella logica $Ł_\infty$ sono precisamente le identità *assolute*, ossia quelle che descrivono coppie di stati di conoscenza σ e τ contenenti la stessa informazione in ogni possibile gioco di Rényi-Ulam. Le sei equazioni (1)-(2) sono esempi di identità assolute—e per di più da esse tutte le identità assolute possono essere ricavate. Un esempio di identità non assoluta è dato da $\sigma \odot \sigma = \sigma$, che esprime la legge di idempotenza della logica classica, e vale precisamente nei giochi di Rényi-Ulam senza bugie.

Chiudendo un circolo di idee, l'analisi logica dei poliedri è solo all'inizio, come mostra il problema aperto della riconoscibilità effettiva dei poliedri *razionali*, dei complessi astratti simpliciali *pesati* e delle MV-algebre *finitamente presentate*.

La confluenza di tecniche geometriche, combinatorie e logico-algebriche su un problema comune è una delle manifestazioni dell'unità della matematica.

BIBLIOGRAFIA

[1] J. W. ALEXANDER, *The combinatorial theory of complexes*, Annals of Mathematics, **31** (1930), 292-320.

[2] E. R. BERLEKAMP, *Block coding for the binary symmetric channel with noiseless, delayless feedback*, In: *Error-correcting Codes*. (Mann, H. B., Ed.,) Wiley, New York (1968), 330-335.

[3] M. BUSANICHE - D. MUNDICI, *Geometry of Robinson consistency in Łukasiewicz logic*, Annals of Pure and Applied Logic, **147** (2007), 1-22.

[4] J. W. S. CASSELS, *An introduction to the geometry of numbers*, Springer, Berlin, 1959.

[5] A. V. CHERNAVSKI and V. P.LEKSINE, *Unrecognizability of manifolds*, Annals of Pure and Applied Logic, **141** (2006), 325-335.

[6] F. CICALESE - D. MUNDICI, *Learning and the art of fault-tolerant guesswork*, Handbook Chapter, In: *Perspectives on Adaptivity and Learning,* I. Stamatescu, et al., Eds., Springer (2003), 115-140.

[7] F. CICALESE - D. MUNDICI - U. VACCARO, *Rota-Metropolis cubic logic and Ulam-Rényi games*, In: *Algebraic Combinatorics and Computer Science: a tribute to Gian-Carlo Rota* (H. Crapo, D. Senato, Eds.), Springer-Verlag (2001), 197-244.

[8] R. CIGNOLI - D. MUNDICI, *Stone duality for Dedekind σ-complete ℓ-groups with order-unit*, Journal of Algebra, **302** (2006), 848-861.

[9] R. L. O. CIGNOLI - I. M. L. D'OTTAVIANO - D. MUNDICI, *Algebraic foundations of many-valued reasoning*, volume 7 of *Trends in Logic*, Kluwer Academic Publishers, Dordrecht (2000).

[10] R. L. O. CIGNOLI - E. J. DUBUC - D. MUNDICI, *Extending Stone duality to multisets and locally finite MV-algebras*, J. Pure and Applied Algebra, **189** (2004), 37-59.

[11] R. CIGNOLI - G. A. ELLIOTT - D. MUNDICI, *Reconstructing C^*-algebras from their Murray von Neumann orders*, Advances in Mathematics, **101** (1993), 166-179,.

[12] P. ERDÖS - P. M. GRUBER - J. HAMMER, *Lattice points*, Pitman Monographs and Surveys in Pure and Applied Mathematics 39, Longman and Wiley, New York, 1989.

[13] G. EWALD, *Combinatorial convexity and algebraic geometry*, Springer-Verlag, New York, 1996.

[14] J. GISPERT - D. MUNDICI - A. TORRENS, *Ultraproducts of $\mathbb{Z}$ with an application to many-valued logics*, Journal of Algebra, **219** (1999), 214-233.

[15] F. HIRZEBRUCH, *Über vierdimensionale Riemannsche Flächen mehrdeutiger analytischer Funktionen von zwei complexen Veränderlichen*, Math. Annalen, **126** (1953), 1-22.

[16] H. W. E. JUNG, *Darstellung der Funktionen eines algebraischen Körpers zweier unabhängigen Veränderlichen x, y in der Umbegung einer Stelle $x = a, y = b$*, J. reine angew. Math., **133** (1908), 289-314.

[17] C. G. LEKKERKERKER, *Geometry of numbers*, Wolters-Noordhoff, Groningen and North-Holland, Amsterdam, 1969.
[18] W. B. R. LICKORISH, *Simplicial moves on complexes and manifolds*, Geometry and Topology Monographs, Vol. 2: Proceedings of the Kirbyfest (1999), 299-320.
[19] C. MANARA- V. MARRA - D. MUNDICI, *Lattice-ordered Abelian groups and Schauder bases of regular fans*, Transactions of the American Mathematical Society, **359** (2007), 1593-1604.
[20] YU. I. MANIN, *A course in mathematical logic,* Springer-Verlag, New York, 1977.
[21] V. MARRA - D. MUNDICI, *The Lebesgue state of a unital abelian lattice-ordered group*, Journal of Group Theory, **10** (2007), 655-684.
[22] P. MCMULLEN, *Valuations and dissections*, In: *Handbook of Convex Geometry,* Vol. **2**. P. M. GRUBER - J. M. WILLS, Eds., Elsevier (1993), 933-988.
[23] R. MORELLI, *The birational geometry of toric varieties*, Journal of Algebraic Geometry, **5** (1996), 751-782.
[24] A. MOSTOWSKI, *L'oeuvre scientifique de Jan Łukasiewicz dans le domaine de la logique mathématique*, Fundamenta Mathematicae, **44** (1957), 1-11.
[25] D. MUNDICI, *Interpretation of AF C^*-algebras in Łukasiewicz sentential calculus*, Journal of Functional Analysis, **65** (1986), 15-63.
[26] D. MUNDICI, *Satisfiability in many-valued sentential logic is NP-complete*, Theoretical Computer Science, **52** (1987), 145-153
[27] D. MUNDICI, *Farey stellar subdivisions, ultrasimplicial groups, and K_0 of AF C^*-algebras*, Advances in Mathematics, **68** (1988), 23-39.
[28] D. MUNDICI, *Logic of infinite quantum systems*, International Journal of Theoretical Physics, **32** (1993), 1941-1955.
[29] D. MUNDICI, *Łukasiewicz normal forms and toric desingularizations*, In: *Proceedings Logic Colloquium '93*, W. Hodges et al., Editors, Oxford University Press, (1996), 401-423.
[30] D. MUNDICI, *Tensor Products and the Loomis-Sikorski theorem for MV-algebras*, Advances in Applied Mathematics, **22** (1999), 227-248.
[31] D. MUNDICI, *Simple Bratteli diagrams with a Gödel incomplete isomorphism problem*, Transactions of the American Mathematical Society, **356** (2004), 1937-1955.
[32] D. MUNDICI, *Representation of σ-complete MV-algebras and their associated Dedekind σ-complete ℓ-groups*, Contemporary Mathematics, **419** (2006), 219-230.
[33] D. MUNDICI, *Bookmaking over infinite-valued events*, International Journal of Approximate Reasoning, **43** (2006), 223-240.
[34] D. MUNDICI, *The Haar theorem for lattice-ordered abelian groups with order-unit*, Discrete and Continuous Dynamical Systems, **21** (2008).
[35] D. MUNDICI - G. PANTI, *Extending addition in Elliott's local semigroup*, Journal of Functional Analysis, **117** (1993), 461-471.
[36] D. MUNDICI - G. PANTI, *Decidable and undecidable prime theories in infinite-valued logic*, Annals of Pure and Applied Logic, **108** (2001), 269-278.
[37] D. MUNDICI - C. TSINAKIS, *Gödel incompleteness in AF C*-algebras*, Forum Mathematicum. In stampa.
[38] M. H. A. NEWMAN, *On the foundations of combinatory analysis situs*, Proc. Royal Academy of Amsterdam, **29** (1926), 610-641.
[39] T. ODA, *Convex bodies and algebraic geometry. An introduction to the theory of toric varieties*, Springer-Verlag, New York, 1988.
[40] G. PANTI, *Dynamical properties of logical substitutions*, Discrete and Continuous Dynamical Systems, **15** (2006), 237-258.

[41] G. PANTI, *Bernoulli automorphisms of finitely generated free MV-algebras*, Journal of Pure and Applied Algebra, **208** (2007), 941-950.
[42] G. PANTI, *Invariant measures in free MV-algebras*, In stampa su Communications in Algebra. http://arxiv.org/abs/math/0508445v2.
[43] A. PELC, *Searching games with errors: fifty years of coping with liars*, Theoretical Computer Science, **270** (2002), 71-109.
[44] A. RÉNYI, *Napló az információelméletröl*, Gondolat, Budapest, 1976. (English translation: *A Diary on Information Theory*, J. Wiley and Sons, New York, 1984).
[45] B. RIEČAN - D. MUNDICI, *Probability on MV-algebras*, In: E. Pap (ed.), *Handbook of Measure Theory*, Vol. II, North-Holland, Amsterdam, (2001), 869-909.
[46] C. P. ROURKE B. J. SANDERSON, *Introduction to piecewise-linear topology*, Springer-Verlag, New York, 1972.
[47] Z. SEMADENI, *Schauder bases in Banach spaces of continuous functions*, Lecture Notes in Mathematics, Springer-Verlag, Berlin, volume 918, 1982.
[48] A. TARSKI - J. Łukasiewicz, *Investigations into the Sentential Calculus*, In: *Logic, Semantics, Metamathematics*, Oxford University Press, 1956, 38-59. Reprinted by Hackett Publishing Company, Indianapolis, 1983.
[49] M. TSUJII, *Absolutely continuous invariant measures for expanding piecewise linear maps*, Invent. Math., **143** (2001), 349-373.
[50] S. ULAM, *Adventures of a Mathematician*, Scribner's, New York, 1976.
[51] H. WEYL, *The elementary theory of convex polyhedra*, In: *Contributions to the theory of games*, Vol. I, Annals of Mathematics Studies 24, University Press, Princeton NJ, 1950, 3-18.
[52] J. WŁODARCZYK, *Decompositions of birational toric maps in blow-ups and blow-downs*. Transactions of the American Mathematical Society, 373-411 (1997), 349.

Dipartimento di Matematica "Ulisse Dini",
Università degli Studi di Firenze, viale Morgagni 67/A, I-50134 Firenze
E-mail: mundici@math.unifi.it

Received January 29, 2008 and in revised form February 15, 2008