South American Journal of Logic
Vol. 2, n. 1, pp. 35–39, 2016
ISSN: 2446-6719

Dickson's Lemma and Higman's Lemma are Equivalent

Josef Berger

Abstract

Dickson's lemma says that for every $f : \mathbb{N} \to \mathbb{N}^n$ there are indices $k < l$ such that $f(k) \leq f(l)$, component-wise. Higman's lemma says that for every sequence (u_i) of binary words there are indices $k < l$ such that u_k is a subword of u_l. We show that these axioms are equivalent in the following sense: given f, we can introduce a sequence (u_i), apply Higman's lemma and find a suitable pair of indices for f. And, vice versa, given (u_n), we can introduce a function f, apply Dickson's lemma and find a suitable pair of indices for (u_i).

We use the variable i for the elements of the set $\{0, 1\}$. Set $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $\mathbb{N}_+ = \{1, 2, 3, \ldots\}$. We use the variables k, l, m, n for the elements of $\mathbb{N}$. The set $\{0, 1\}^*$ of finite binary words is defined inductively by

$$\frac{}{() \in \{0,1\}^*} \qquad \frac{u \in \{0,1\}^*}{ui \in \{0,1\}^*}\,.$$

Here $()$ stands for the empty word. The length $|u|$ of $u \in \{0, 1\}^*$ is given by

$$|()| = 0 \qquad |ui| = |u| + 1\,.$$

We define the subword relation $\sqsubseteq$ on $\{0, 1\}^*$ by

$$() \sqsubseteq ()$$

$$\frac{u \sqsubseteq w}{u \sqsubseteq w0} \qquad \frac{u \sqsubseteq w}{u \sqsubseteq w1}$$

$$\frac{u \sqsubseteq w}{u0 \sqsubseteq w0} \qquad \frac{u \sqsubseteq w}{u1 \sqsubseteq w1}\,.$$

Higman's lemma [2] is the following axiom.

HL For every function $g : \mathbb{N} \to \{0, 1\}^*$ there are k, l such that

- $k < l$
- $g(k) \sqsubseteq g(l)$.

Dickson's lemma [1] is the following axiom.

DL For every n and every $f : \mathbb{N} \to \mathbb{N}^n$ there are k, l such that

- $k < l$
- $f(k) \leq f(l)$ (component-wise) .

Proposition 1 *The axioms* DL *and* HL *are equivalent.*

In order to prove this proposition, we work with slightly altered but obviously equivalent versions of the axioms.

HL' For every function $g : \mathbb{N} \to \{0,1\}^*_0$ there are k, l such that

- $k < l$
- $g(k) \sqsubseteq g(l)$,

where $\{0,1\}^*_0$ is given by

$$\frac{}{0 \in \{0,1\}^*_0} \qquad \frac{u \in \{0,1\}^*_0}{ui \in \{0,1\}^*_0} .$$

DL' For every n and every $f : \mathbb{N} \to \mathbb{N}^n_+$ there are k, l such that

- $k < l$
- $f(k) \leq f(l)$ (component-wise).

Define $\lambda : \{0,1\}^*_0 \to \{0,1\}$ by

$$\lambda(0) = 0 \qquad \lambda(ui) = i .$$

For every $u \in \{0,1\}^*_0$ we define $\Phi(u)$ by

$$\Phi(0) = 1 \qquad \Phi(ui) = \begin{cases} \Phi(u) & \text{if } \lambda(u) = i \\ \Phi(u) + 1 & \text{if } \lambda(u) \neq i \end{cases} .$$

$\Phi(u)$ is called the *weight* of u. Next, we define a bijection

$$F : \{0,1\}^*_0 \to \cup_{m \geq 1} \mathbb{N}^m_+ .$$

Set $F(0) = (1)$ and suppose that $F(u) = (k_1, \ldots, k_m)$. Set

$$F(ui) = \begin{cases} (k_1, \ldots, k_m + 1) & \text{if } \lambda(u) = i , \\ (k_1, \ldots, k_m, 1) & \text{if } \lambda(u) \neq i . \end{cases}$$

Fix $n \in \mathbb{N}_+$. Let $\mathcal{W}_n$ denote the elements of $\{0,1\}^*_0$ with weight n. Let F_n be the restriction of F to $\mathcal{W}_n$.

Lemma 2 *$F_n : \mathcal{W}_n \to \mathbb{N}_+^n$ is bijective and order-preserving.*

Define $G_n : \cup_{m\geq 1}\mathbb{N}_+^m \to \mathbb{N}_+^n$ by

$$G_n(k_1,\ldots,k_m) = \begin{cases} (k_1,\ldots,k_m,1,\ldots,1) & \text{if } m < n\,, \\ (k_1,\ldots,k_n) & \text{if } n \leq m\,. \end{cases}$$

For $u \in \{0,1\}_0^*$ set

$$u!_n = F_n^{-1}(G_n(F(u))).$$

Note that

- $\Phi(u!_n) = n$
- if $\Phi(u) = n$ then $u!_n = u$
- if $\Phi(u) < n$ then $u!_n$ is the shortest extension of u with weight n
- if $\Phi(u) > n$ then $u!_n$ is the largest restriction of u with weight n
- if $\Phi(u) > n$ then $|u!_n| < |u|$.

Lemma 3 *For all u, w in $\{0,1\}_0^*$ we have*

$$(2\cdot|u| \leq \Phi(w)) \;\Rightarrow\; u \sqsubseteq w\,.$$

Proof. In order to avoid nested induction, we prove the decidable formula

$$\forall u,w \in \{0,1\}_0^*\,(|u| \leq k \;\wedge\; |w| \leq k \;\wedge\; (2\cdot|u| \leq \Phi(w)) \;\Rightarrow\; u \sqsubseteq w)\,,$$

by induction on k. For $k = 1$, there is nothing to prove. Now assume that the formula holds for $k \in \mathbb{N}_+$. Fix $u, w \in \{0,1\}_0^*$ such that

$$|u| \leq k+1 \;\wedge\; |w| \leq k+1 \;\wedge\; (2\cdot|u| \leq \Phi(w))$$

holds. We can assume that $u = vi$ for some $v \in \{0,1\}_0^*$. Set $l = 2\cdot|v|$. Note that $2\cdot|v| = \Phi(w!_l)$. Therefore, the induction hypothesis implies that $v \sqsubseteq w!_l$, thus we can conclude that $u \sqsubseteq w$. ■

Lemma 4

$$G_n(F(u)) = F_n(u!_n)\,.$$

Lemma 5 *Fix* $u, w \in \{0,1\}_0^*$ *with*

$$\Phi(u) \leq \Phi(w) \leq n \quad \textit{and} \quad u!_n \sqsubseteq w!_n \,.$$

Then we have

$$u \sqsubseteq w.$$

Proof. Set $k = \Phi(u)$. The assumption $u!_n \sqsubseteq w!_n$ implies $G_n(F(u)) \leq G_n(F(w))$ and therefore

$$F_k(u) = G_k(F(u)) \leq G_k(F(w)) = F_k(w!_k).$$

Thus we obtain

$$u \sqsubseteq w!_k.$$

Since $k \leq \Phi(w)$, we obtain $w!_k \sqsubseteq w$ and therefore $u \sqsubseteq w$. ■

"HL' ⇒ DL'"

Fix $n \in \mathbb{N}_+$ and $f : \mathbb{N} \to \mathbb{N}_+^n$. Applying HL to $F_n^{-1} \circ f$ yields $k < l$ with

$$F_n^{-1} \circ f(k) \sqsubseteq F_n^{-1} \circ f(l),$$

which implies $f(k) \leq f(l)$.

"DL' ⇒ HL'"

Fix $g : \mathbb{N} \to \{0,1\}_0^*$. Set $n = 2 \cdot |g(0)|$. Then DL yields $k < l$ in $\mathbb{N}$ such that

$$(F_n(g(k)!_n), \Phi(g(k))) \leq (F_n(g(l)!_n), \Phi(g(l)))\,.$$

If $n < \Phi(g(l))$, we obtain $g(0) \sqsubseteq g(l)$ by Lemma 3. Otherwise, we have

$$\Phi(g(k)) \leq \Phi(g(l)) \leq n \quad \text{and} \quad g(k)!_n \sqsubseteq g(l)!_n.$$

Thus $g(k) \sqsubseteq g(l)$ by Lemma 5.

Remark 6 *This result is of combinatorial nature. However, we work within intuitionistic logic (the law of excluded middle is not applied) and use inductive proofs only for quantifier-free formulas. Moreover, we do not use any instance of the axiom of choice. Therefore, results on Dickson's lemma correspond to results on Higman's lemma, in any formal system which allows the definition of the basic string operations, like Heyting Arithmetic. To see that Dickson's lemma and Higman's lemma are practically the same statements is of interest even though it is well-known that both are provable within intuitionistic logic [3, 4].*

References

[1] Leonard Eugene Dickson, 'Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors.' *Am. J. Math* 35 (1913), 413–422

[2] Graham Higman, 'Ordering by Divisability in Abstract Algebras.' *Proc. London Math. Soc.* s3-2 (1) (1952) , 326-336

[3] Stephen G. Simpson, 'Ordinal numbers and the Hilbert basis theorem.' *The Journal of Symbolic Logic* 53 no. 3 (1988), 961–974

[4] Wim Veldman, 'An intuitionistic proof of Kruskal's theorem.' *Arch. Math. Logic* 43 (2004), 215–264

Josef Berger
Mathematisches Institut
Ludwig-Maximilians-Universität München
Theresienstraße 39, 80333 München, Germany
E-mail: `jberger@math.lmu.de`