Wooley's Discrete Inequality

Angeliki Koutsoukou-Argyraki
Royal Holloway, University of London and University of Cambridge

March 17, 2025

Abstract

This is a formalisation of the proof of an inequality by Trevor D. Wooley attesting that when $\lambda > 0$,

$$\min_{r \in \mathbb{N}} (r + \lambda/r) \leq \sqrt{4\lambda + 1}$$

with equality if and only if $\lambda = m(m-1)$ for some positive integer m.

Contents

1 Wooley's Discrete Inequality

theory *Wooley-Elementary-Discrete-Inequality*
imports *HOL−Library.Quadratic-Discriminant HOL−Real-Asymp.Real-Asymp*

begin

This is a formalisation of the proof of an inequality by Trevor D. Wooley attesting that when $\lambda > 0$,

$$\min_{r \in \mathbb{N}} (r + \lambda/r) \leq \sqrt{4\lambda + 1}$$

with equality if and only if $\lambda = m(m-1)$ for some positive integer m. The source is the note "An Elementary Discrete Inequality" available on Wooley's webpage [1]: https://www.math.purdue.edu/~twooley/publ/20230410discineq.pdf.

1.1 General elementary technical lemmas

```
lemma obtains-nat-in-interval:
  fixes x::real assumes x≥0
  obtains c::nat where c ∈ {x<.. x+1}
proof
  show nat⌊x+1⌋ ∈ {x<..x + 1}
    using assms by force
qed

lemma obtains-nat-in-interval-greater-leq:
  fixes x::real assumes x≥0
  obtains c::nat where c >x and c ≤ x+1
  by (meson assms greaterThanAtMost-iff obtains-nat-in-interval)

lemma obtains-nat-in-interval-half:
  fixes x::real assumes x≥1/2
  obtains c::nat where c > x − (1/2) and c ≤ x+1/2
  using assms  obtains-nat-in-interval-greater-leq [of x−1/2]
  by (smt (verit) field-sum-of-halves)
```

1.2 Trivial case, where we minimise over all positive real values of r

```
theorem elementary-ineq-Wooley-real:
  fixes l::real and g::real ⇒ real
  assumes l>0 and ∀ r ∈ R. g r = r+(l/r)
    and R={r::real. r>0}
  shows (∀ r ∈ R. g r ≥  2∗ sqrt(l)) ∧ (∀ r ∈ R. g (sqrt(l)) ≤ g r)
proof−
  have ∀ r ∈ R. 2 ∗ sqrt(l)+ (sqrt(r) − (sqrt(l)/sqrt(r)))^2 = r+(l/r)
    using  assms  by (simp add: power-divide power2-diff)
  moreover
  have ∀ r ∈ R. 2 ∗ sqrt(l)+ (sqrt(r) − (sqrt(l)/sqrt(r)))^2 ≥ 2 ∗(sqrt(l))
    using assms by auto
  ultimately have ∀ r ∈ R. r+(l/r) ≥ 2∗sqrt(l) by simp
  moreover
  have g (sqrt(l)) = 2 ∗sqrt(l) using assms by (simp add: real-div-sqrt)
  ultimately show  ?thesis using assms by auto
qed
```

1.3 Main result: Inequality for the discrete version

```
theorem elementary-discrete-ineq-Wooley:
  fixes l::real and g::nat ⇒ real
  assumes l>0 and R = {r::nat. r>0} and ∀ r ∈ R. g r = r+ (l/r)
  shows (INF r ∈ R. g r) ≤ sqrt(4∗l+1)

proof−
```

We will first show the inequality for a specific choice of $r_u \in R$. Then the assertion of the theorem will be simply shown by transitivity.

```
define x::real where x = sqrt(l+1/4)
with assms have x>1/2
  by (smt (verit, best) real-sqrt-divide real-sqrt-four real-sqrt-less-iff real-sqrt-one)

obtain r-u::nat where r-u >x −1/2 and r-u ≤ x+1/2
  using obtains-nat-in-interval-half ‹x>1/2› by (metis less-eq-real-def)
have r-u ∈ R using assms ‹1 / 2 < x› ‹x − 1 / 2 < real r-u› by auto
have ru-gt: r-u > sqrt(l+1/4)−1/2 using ‹r-u >x −1/2› ‹x =sqrt(l+1/4)›
by blast
have ru-le: r-u ≤ sqrt(l+1/4)+1/2 using ‹r-u ≤ x +1/2› ‹x =sqrt(l+1/4)›
by blast
```

Proving the following auxiliary statement is the key part of the whole proof.

```
have auxiliary: |r-u − (l/r-u)| ≤ 1
proof−
  define δ::real where δ = r-u − sqrt(l+1/4)
  with assms ru-gt δ-def ru-le
  have δ: δ > −1/2 δ ≤ 1/2
    by auto

  have a: |r-u − l/r-u| = | ((sqrt(l+1/4) + δ)^2 −l)/(sqrt(l+1/4) + δ)|
    using δ-def
    by (smt (verit, ccfv-SIG) ‹1 / 2 < x› ‹x − 1 / 2 < real r-u›
        add-divide-distrib nonzero-mult-div-cancel-right power2-eq-square)

  have b:| ((sqrt(l+1/4) + δ)^2 −l)/(sqrt(l+1/4) + δ)| =
|2∗ δ +( ((1/4) − δ^2)/(sqrt(l+1/4) + δ ))|
  proof−
    have |((sqrt(l+1/4) + δ)^2 −l)/(sqrt(l+1/4) + δ) | =
 |(1/4 + 2∗(sqrt(l+1/4))∗ δ+ δ^2)/(sqrt(l+1/4) + δ) |
    by (smt (verit, best) assms(1) divide-nonneg-nonneg power2-sum real-sqrt-pow2)
    also have ... = | ( 2∗ δ∗ (sqrt(l+1/4))+ 2∗ δ^2 + 1/4 −δ^2 )/(sqrt(l+1/4)
+ δ)|
      by (smt (verit) power2-sum)
     also have ... = | ( 2∗ δ∗ (sqrt(l+1/4)+ δ) + 1/4 −δ^2 )/(sqrt(l+1/4) +
δ)|
      by (smt (verit, ccfv-SIG) power2-diff power2-sum)
    also have ... = | ( 2∗ δ∗ (sqrt(l+1/4)+ δ))/(sqrt(l+1/4) + δ)
+ ((1/4 −δ^2 )/(sqrt(l+1/4) + δ)) |
      by (metis add-diff-eq add-divide-distrib)
    also have ... = | 2∗ δ + ((1/4 −δ^2 )/(sqrt(l+1/4) + δ)) |
      using ‹δ = real r-u − sqrt (l + 1 / 4)› ‹r-u ∈ R› assms by force
    finally show ?thesis .
  qed

  show ?thesis
```

We distinguish the cases $\delta > 0$ and $\delta \leq 0$:

```
proof (cases δ > 0)
  case True
  define t::real where t = 1/2 − δ
  have c: 0 ≤ 2∗ δ +(( 1/4 − δ^2)/(sqrt(l+1/4) + δ ))
  proof−
    have δ^2 ≤ 1/4 using δ ‹δ > 0›
      by (metis less-eq-real-def plus-or-minus-sqrt real-sqrt-divide real-sqrt-four
real-sqrt-le-iff real-sqrt-one real-sqrt-power)
    then have 1/4 −δ^2 ≥ 0
      by simp
    then show ?thesis using ‹δ > 0› assms by simp
  qed

    have d: 2∗ δ +( (1/4 − δ^2)/(sqrt(l+1/4) + δ )) ≤ 1 −2∗t + ((t−t^2)/
(1−t))
  proof−
    have δ = 1/2 − t using t-def by simp
    then have 2∗ δ +( (1/4 − δ^2)/(sqrt(l+1/4) + δ )) =
           2∗(1/2 − t ) +( (1/4 − ( 1/2 − t)^2)/(sqrt(l+1/4) + 1/2 − t
))
      by simp
   also have ... = 1 − 2∗t + ( (1/4 − ( 1/4 −2∗(1/2)∗ t+ t^2))/(sqrt(l+1/4)
+ 1/2 − t ))
      by (simp add: power2-diff power-divide)
    also have ... = 1 − 2∗t + ((t− t^2)/(sqrt(l+1/4) + 1/2 − t )) by simp
    also have ... ≤ 1 −2∗t + ((t−t^2)/ (1−t))
    proof−
      have sqrt(l+1/4) + 1/2 ≥ 1
        using ‹1/2 < x› x-def by linarith
      then have ∗: sqrt(l+1/4) + 1/2 −t ≥ 1 −t by simp
      have 1−t ≠ 0 using ‹t = 1/2 − δ› ‹δ >0› by linarith
      have sqrt(l+1/4) + 1/2 −t ≠ 0
        using δ-def ‹t = 1/2 − δ› ‹δ >0› assms(1) by force
      then have (1/(sqrt(l+1/4) + 1/2 − t ))≤ (1/ (1−t))
          using ∗ ‹1−t ≠ 0 › by (smt (verit) True ‹δ = 1/2 − t› frac-le
le-divide-eq-1-pos)
      have t−t^2 ≥0 using ‹δ = 1/2 − t› ‹δ >0›
        by (smt (verit, best) ‹δ ≤ 1 / 2› field-sum-of-halves le-add-same-cancel1
nat-1-add-1
          power-decreasing-iff
        power-one-right real-sqrt-pow2-iff real-sqrt-zero zero-less-one-class.zero-le-one)
      then have ((t−t^2) /(sqrt(l+1/4) + 1/2 − t ))≤ ((t−t^2)/ (1−t))
        by (smt (verit) ∗ True ‹t = 1/2 − δ› frac-le le-divide-eq-1-pos)
      then show ?thesis by force
    qed
    finally show ?thesis .
  qed
```

```
    have e: 1 −2∗t + ((t−t²)/ (1−t)) ≤ 1
    proof−
     have 1 −2∗t + ((t−t²)/ (1−t)) =  1−2∗t + ((1−t)∗t /(1−t)) by algebra
      also have . . . =  1− t
        using c d by fastforce
      finally show ?thesis
        using δ t-def by linarith
    qed

    show ?thesis using a b c d e by linarith

  next
    case False
    define t::real where t = 1/2 + δ
    then have δ = t−1/2by simp
    have δ ≤ 0 using False by auto

    have −( 2∗ δ +( ((1/4) − δ²)/(sqrt(l+1/4) + δ ))) =
− ( 2∗ (t−1/2) +( ((1/4) − (t−1/2)^2)/(sqrt(l+1/4) + t − 1/2 )))
      using ‹δ = t−1/2›  by auto

    also have . . . =−( 2∗t− 1 +( (  t−t²)/(sqrt(l+1/4) + t − 1/2 )))
      by (simp add: power2-diff power-divide)

    finally have ∗∗∗: −( 2∗ δ +( ((1/4) − δ²)/(sqrt(l+1/4) + δ ))) =
−( 2∗t− 1 +( (  t−t²)/(sqrt(l+1/4) + t − 1/2 ))) .

    have c:−( 2∗ δ +( ((1/4) − δ²)/(sqrt(l+1/4) + δ ))) ≤ 1 −2∗t − ((t−t²)/
(sqrt(l+1/4)))
    proof−
      have  c1: sqrt(l+1/4) + t − 1/2 ≤ sqrt(l+1/4)
        using ‹δ = t − 1 / 2› ‹δ ≤ 0› by simp

      have (sqrt(l+1/4) + t − 1/2) ≠ 0  sqrt(l+1/4) ≠ 0
        using assms δ-def ‹δ = t − 1/2› ‹r-u ∈ R› by auto
      then
      have c2: (t−t²)/(sqrt(l+1/4) + t − 1/2) ≥(t−t²)/ sqrt(l+1/4)
        using c1 assms
        by (smt (verit, best) δ-def ru-gt ‹t = 1/2 + δ›
          field-sum-of-halves frac-le le-add-same-cancel1 nat-1-add-1 of-nat-0-le-iff

            power-decreasing-iff power-one-right zero-less-one-class.zero-le-one)

      have c3: − (t−t²)/(sqrt(l+1/4) + t − 1/2) ≤ − (t−t²)/ sqrt(l+1/4)
        using c2  by linarith
      show ?thesis using ∗∗∗ c3 by linarith

    qed
```

```
have d: 1 −2∗t − ((t−t²)/ (sqrt(l+1/4))) ≤ 1
proof−
  have ∗: t >0 using ‹δ > −1/2›  ‹t = 1/2 + δ› by simp
  have ∗∗: t ≤ 1 using  ‹δ ≤ 0› ‹t = 1/2 + δ› by simp
  show ?thesis using ∗ ∗∗
       by (smt (verit) assms(1) divide-nonneg-nonneg mult-le-cancel-right2
power2-eq-square real-sqrt-ge-0-iff)
qed

have e: −( 2∗ δ +( ((1/4) − δ²)/(sqrt(l+1/4) + δ ))) ≥ 1 −2∗t − ((t−t²)/t)

proof−
  have −( 2∗ δ +( ((1/4) − δ²)/(sqrt(l+1/4) + δ )))
= −( 2∗t− 1 +((t−t²)/(sqrt(l+1/4) + t − 1/2)))
    using ∗∗∗ by simp

  have ( (  t−t²)/(sqrt(l+1/4) + t − 1/2 )) ≤ (t−t²)/ t
  proof−
    have †: (sqrt(l+1/4) + t − 1/2 ) ≥  t using assms
     by (smt (verit, best) one-power2 power-divide real-sqrt-four real-sqrt-pow2
sqrt-le-D)
    moreover have t >0 using ‹ δ > −1/2›  ‹t = 1/2 + δ› by simp
    ultimately have (sqrt(l+1/4) + t − 1/2 ) >0
      by auto
    show ?thesis using † ‹(sqrt(l+1/4) + t − 1/2 ) >0›
        ‹0 < t›
      by (smt (verit, best) ‹δ ≤ 0› ‹t = 1/2 + δ›
      frac-le le-add-same-cancel1 le-divide-eq-1-pos nat-1-add-1 power-decreasing-iff

          power-one-right zero-less-one-class.zero-le-one)
  qed
  with ∗∗∗ show ?thesis by linarith

qed
have f: 1 −2∗t − ((t−t²)/t) ≥ −1/2
proof−
  have t >0 using ‹ δ > −1/2›  ‹t = 1/2 + δ› by simp
  then have 1 −2∗t − ((t−t²)/t) = 1−2∗t −(1 −t)
    by (metis divide-diff-eq-iff less-irrefl one-eq-divide-iff power2-eq-square)
  also have . . . = −t by auto
  finally show ?thesis
    using ‹δ ≤ 0› ‹t = 1/2 + δ›  by linarith
qed
show ?thesis using a b c d e f by linarith
qed
qed
```

The next step is to show that by the statement named "auxiliary" shown above, we can directly show the desired inequality for the specific $r_u \in R$:

```
  have (r-u − l/r-u)^2 ≤1
    using auxiliary abs-square-le-1 by blast
  then have (r-u^2 − 2∗r-u∗ (l/r-u) + l^2/r-u^2 ≤1)
    using power2-diff power-divide assms
    by (smt (verit) mult-2 of-nat-add of-nat-eq-of-nat-power-cancel-iff)
  then have r-u^2 − 2∗l + l^2/r-u^2 ≤1 using assms ‹r-u ∈ R› by force
  then have r-u^2 + 2∗l + l^2/r-u^2 ≤ ( 4∗l+1) by argo
   then have r-u^2 + 2∗r-u∗(l/r-u) + l^2/r-u^2 ≤ ( 4∗l+1) using assms by
simp
  then have (r-u+ (l/r-u))^2 ≤ ( 4∗l+1)
   by (smt (verit, best) mult-2 of-nat-add of-nat-power-eq-of-nat-cancel-iff power2-sum

        power-divide)
  then have (r-u+ (l/r-u)) ≤ sqrt(4∗l+1) using real-le-rsqrt by blast
  moreover
```

The following shows that it is enough that we showed the inequality for the specific $r_u \in R$, as the statement of the theorem will then simply hold by transitivity.

```
  have (INF r ∈ R. g r) ≤ g r-u
  proof−
    have bdd-below (g ‘ R) unfolding bdd-below-def
      using  assms image-iff
     by (metis add-increasing assms(1) divide-nonneg-nonneg image-iff less-eq-real-def
          of-nat-0-le-iff)
    show ?thesis
      by (simp add: ‹bdd-below (g ‘ R)› ‹r-u ∈ R› cINF-lower)
  qed
  ultimately show ?thesis using assms ‹r-u ∈ R› by force
qed
```

1.4 Special case: Equality for the discrete version

We will now show a special case of the main result where equality holds instead of inequality.

We will need to make use of the following technical lemma, which will be used so as to guarantee that there exists a $p \in R$ for which the INF of $g(r)$ equals to $g(p)$. To this end, we will show that here the infimum INF can be identified with the minimum Min by restricting to a finite set. As the operator Min in Isabelle is used for finite sets and R is infinite, we used INF in the original formulation, however here Min and INF can be identified.

The following technical lemma is by Larry Paulson:

```
lemma restrict-to-min:
  fixes l::real and g::nat ⇒ real
  assumes l>0 and R-def: R={r::nat. r>0} and g-def: ∀ r. g r = r + (l/r)
  obtains F where finite F F ⊆ R (INF r ∈ R. g r) = Min (g ‘ F) F ≠ {}
```

```
proof −
  have ge0: g r ≥ 0 for r
    using ‹l>0› R-def g-def  by (auto simp: g-def)
  then have bdd: bdd-below (g ‘ R)
    by (auto simp add: g-def R-def bdd-below-def)
  have ∀F n in sequentially. g 1 < g n
    by (simp add: g-def) real-asymp
  then obtain N where N>0 and N: ⋀r. r≥N ⟹ g 1 < g r
    by (metis Suc-leD eventually-sequentially less-Suc-eq-0-disj)
  define F where F = R ∩ {..N}
  have F: finite F F ⊆ R
    by (auto simp add: F-def)
  have F ≠ {}
    using F-def R-def ‹0 < N› by blast
  have (INF r ∈ R. g r) = (INF r ∈ F. g r)
  proof (intro order.antisym cInf-mono bdd)
    show bdd-below (g ‘ F)
      by (meson ge0 bdd-belowI2)
  next
    fix b
    assume b ∈ g ‘ R
    then show ∃ a∈g ‘ F. a ≤ b
      unfolding image-iff F-def R-def Bex-def
    by (metis N linorder-not-less IntI atMost-iff mem-Collect-eq nle-le zero-less-one)
  qed (use ‹F⊆R› ‹0 < N› in ‹auto simp: R-def F-def›)
  also have ... = Min (g ‘ F)
    using ‹F ≠ {}› by (simp add: ‹finite F› cInf-eq-Min)
  finally have (INF r ∈ R. g r) = Min (g ‘ F) .
  with F show thesis
    using that ‹F ≠ {}› by blast
qed
```

We will make use of the following calculation, which is convenient to formulate separately as a lemma.

```
lemma elementary-discrete-ineq-Wooley-quadratic-eq-sol:
  fixes l::real and g::nat ⇒ real
  assumes l>0 and ∀ r. g r =r+ (l/r) and g r = sqrt(4*l+1)
   shows (r = 1/2 + (1/2)* sqrt( 4*l +1)) ∨ (r = − 1/2 + (1/2)* sqrt(4*l
+1))
proof−
  have eq0: r^2 − r*(sqrt( 4*l+1 )) + l = 0
  proof−
    have r*( r + l/r) = r*(sqrt(4*l+1)) using assms by simp
    then have  r^2 + r*(l/r) = r*(sqrt(4*l+1))
      by (simp add: distrib-left power2-eq-square)
    then show ?thesis
     by (smt (verit, ccfv-threshold) assms divide-eq-eq mult.commute real-sqrt-gt-1-iff)
  qed
```

Solving the above quadratic equation gives the following two roots:

have *roots*:$(r = 1/2 + (1/2)*sqrt(\ 4*l +1)) \vee (r = -\ 1/2 + (1/2)*sqrt(4*l+1))$
proof−
define *a*::*real* **where** $a = 1$
define *b*::*real* **where** $b = -\ sqrt(4*l+1)$
define *c*::*real* **where** $c = l$
have $a*r\hat{\ }2 + b*\ r + c = 0$ **using** *eq0* **by** (*simp add*: *mult.commute a-def b-def c-def*)
then have *A*: $(r = (-b + sqrt(\ discrim\ a\ \ b\ c))/\ 2*a) \vee (r = (-b - sqrt(\ discrim\ a\ \ b\ c))/\ 2*a)$
using *discriminant-iff*[*of a r*] *a-def* **by** *simp*
have $discrim\ a\ b\ c = b\hat{\ }2 - 4*a*c$
using *discrim-def* **by** *simp*
then have *B*: $(r = (-b + sqrt(b\hat{\ }2 - 4*a*c))/\ 2*a) \vee (r = (-b - sqrt(b\hat{\ }2 - 4*a*c))/\ 2*a)$
using *A* **by** *auto*
then have *C*: $(r = (-b + sqrt(b\hat{\ }2 - 4*c))/\ 2) \vee (r = (-b - sqrt(b\hat{\ }2 - 4*c))/\ 2)$
using *a-def* **by** *simp*
have $b\hat{\ }2 - 4*c = 1$ **using** *b-def c-def assms*(*1*) **by** *auto*
then have $(r = (-b + 1)/\ 2) \vee (r = (-b - 1)/\ 2)$
using *C* **by** *auto*
then show *?thesis* **using** *b-def* **by** *auto*
qed
show *?thesis* **using** *roots* **by** *simp*
qed

The special case with equality involves a double implication (iff), and we start by showing one direction.

theorem *elementary-discrete-ineq-Wooley-special-case-1*:
fixes *l*::*real* **and** *g*::*nat* ⇒ *real* **assumes** $l>0$ **and** $R=\{r::nat.\ r>0\}$ **and** $\forall\ r.\ g\ r = r + (l/r)$
and $(INF\ r \in R.\ g\ r) = sqrt(4*l+1)$
shows $\exists\ m::nat.\ l = m*(m-1)$

proof−
have $\exists\ p \in R.\ (INF\ r \in R.\ g\ r) = g\ p$
proof−
obtain *F* **where** ∗:‹$(INF\ r \in R.\ g\ r) = Min\ (g\ `\ F)$› **and** ‹*finite F*› **and** ‹$F \subseteq R$› ‹$F \neq \{\}$›
using *assms restrict-to-min* **by** *metis*
then obtain *p*::*nat* **where** $Min\ (g\ `\ F) = g\ p\ \ p \in R$
by (*smt* (*verit*) *Min-in finite-imageI image-iff image-is-empty subsetD*)
with ∗ **show** *?thesis* **by** *metis*
qed
with *assms*
obtain *r-u*::*nat* **where** g *r-u* $= sqrt(4*l+1)$ **and** *r-u* $\in R$
by *metis*
then have *ru*: (*r-u* + (*l*/*r-u*)) $= sqrt(\ 4*l+1\ )$
using *assms* **by** *auto*

have (*r-u* = 1/2 + (1/2)∗ *sqrt*(4∗*l* +1)) ⟹ (*l* = *r-u*^2 − *r-u*)
proof−
assume *r-u* = 1/2 + (1/2)∗ (*sqrt*(4∗*l* +1))
then have 2∗ *r-u* = 1 + *sqrt*(4∗*l* +1) **by** *simp*
then have (2∗ *real*(*r-u*) −1)^2 = (4∗*l* +1) **using** *assms* **by** *auto*
then have (2∗*real*(*r-u*))^2 −2∗(2∗*real*(*r-u*)) +1 = (4∗*l* +1)
by (*simp add*: *power2-diff*)
then have 4∗*real*(*r-u*)^2−4∗(*r-u*) = 4∗*l* **by** *fastforce*
then show (*l* = *r-u*^2 − *r-u*)
by (*simp add*: *of-nat-diff power2-eq-square*)
qed
moreover
have (*r-u* = − 1/2 + (1/2)∗ *sqrt*(4∗*l* +1))⟹ (*l* =*r-u*^2 + *r-u*)
proof−
assume *r-u* = − 1/2 + (1/2)∗ *sqrt*(4∗*l* +1)
then have 2 ∗ *r-u* +1 = *sqrt*(4∗*l*+1) **by** *simp*
then have (2∗*r-u* +1)^2 = (4∗*l*+1) **using** *assms* **by** *auto*
then have 4∗(*r-u*)^2 +4∗*r-u* +1 = 4∗*l*+1
by (*simp add*: *power2-eq-square*)
then show (*l* =*r-u*^2 + *r-u*)
by (*simp add*: *of-nat-diff power2-eq-square*)
qed
moreover
have (*r-u* = 1/2 + (1/2)∗ *sqrt*(4∗*l* +1)) ∨ (*r-u* = − 1/2 + (1/2)∗ *sqrt*(4∗*l* +1))
using *assms ru elementary-discrete-ineq-Wooley-quadratic-eq-sol*
assms **by** *auto*
ultimately have (*l* =*r-u*^2 + *r-u*) ∨ (*l* = *r-u*^2 − *r-u*)
by *blast*
then show *?thesis*
by (*metis add-implies-diff distrib-left mult.commute mult.right-neutral power2-eq-square right-diff-distrib′*)

(Interestingly, the above use of metis finished the proof in a simple step guaranteeing the existence of a witness with the desired property).

qed

Now we show the other direction.

theorem *elementary-discrete-ineq-Wooley-special-case-2*:
fixes *l*::*real* **and** *g*::*nat* ⇒ *real*
assumes *l*>0 **and** *R*={*r*::*nat*. *r*>0} **and** ∀ *r*. *g r* =*r*+ (*l*/*r*) **and** ∃ *m*::*nat*. *l* =*m*∗(*m*−1)
shows (*INF r* ∈ *R*. *g r*) = *sqrt*(4∗*l*+1)

proof−

obtain *r-u*::*nat* **where** (*l* =*r-u*^2 + *r-u*) **using** *assms*
by (*metis add.commute add-cancel-left-right mult-eq-if power2-eq-square*)

then have *sqrt(4∗l +1)= sqrt(4∗r-u^2 +4∗ r-u +1)* **by** *simp*
moreover have *4∗r-u^2 +4∗ r-u +1 =(2∗r-u +1)^2*
by (*simp add*: *Groups.mult-ac*(*2*) *distrib-left power2-eq-square*)
ultimately have *4*: *sqrt(4∗l +1)= sqrt((2∗r-u +1)^2)* **by** *metis*
then have *ru*: *r-u = −1/2 + 1/2∗sqrt(4∗l +1)* **by** (*simp add*: *add-divide-distrib*)

To prove the conclusion of the theorem, we will follow a proof by contradiction.

show *?thesis*
proof (*rule ccontr*)
assume *Inf* (*g ‘ R*) ≠ *sqrt* (*4* ∗ *l* + *1*)
then have *inf*: (*INF r* ∈ *R*. *g r*) < *sqrt*(*4*∗*l*+*1*)
using *assms less-eq-real-def elementary-discrete-ineq-Wooley* **by** *blast*

have ∃ *p* ∈ *R*. (*INF r* ∈ *R*. *g r*) = *g p*
proof−
obtain *F* **where** ∗:‹(*INF r* ∈ *R*. *g r*) = *Min* (*g ‘ F*)› **and** ‹*finite F*› ‹*F* ⊆ *R*› ‹*F* ≠ {}›
using *assms restrict-to-min* **by** *metis*
then obtain *p*::*nat* **where** *Min* (*g ‘ F*) = *g p* *p* ∈ *R*
by (*meson Min-in finite-imageI imageE image-is-empty subsetD*)
with ∗ **show** *?thesis* **by** *metis*
qed

obtain *p*::*nat* **where** *p* ∈ *R* **and** (*INF r* ∈ *R*. *g r*) = *g p* **using** *assms*
‹∃ *p* ∈ *R*. (*INF r* ∈ *R*. *g r*) = *g p*› **by** *blast*
then have (*p*+ *l*/*p* < *sqrt*(*4*∗*l*+*1*))
using *inf assms*(*3*) **by** *auto*

have *p*∗(*p*+ *l*/*p*) < *p*∗(*sqrt*(*4*∗*l*+*1*))
using ‹*p* ∈ *R*› ‹(*p*+ *l*/*p* < *sqrt*(*4*∗*l*+*1*))› *assms* **by** *simp*
then have *p^2* − *p*∗(*sqrt*(*4*∗*l*+*1*))+ *l*<*0*
by (*smt* (*verit*) ‹*p* ∈ *R*› *assms*(*2*) *distrib-left mem-Collect-eq nonzero-mult-div-cancel-left*
of-nat-0-less-iff of-nat-mult power2-eq-square times-divide-eq-right)

We now need to find the possible values of this hypothetical $p \in R$, i.e. the roots of the above quadratic inequality. (These will be in-between the roots of the corresponding quadratic equation which were given in lemma ⟦*0* < *?l*; ∀ *r*. *?g r* = *real r* + *?l* / *real r*; *?g ?r* = *sqrt* (*4* ∗ *?l* + *1*)⟧ ⟹ *real ?r* = *1* / *2* + *1* / *2* ∗ *sqrt* (*4* ∗ *?l* + *1*) ∨ *real ?r* = − *1* / *2* + *1* / *2* ∗ *sqrt* (*4* ∗ *?l* + *1*)). Here we show that the roots of the quadratic inequality lie in the following interval via a direct calculation:

have *p*: (*p* < (*sqrt*(*4*∗*l*+*1*) + *1*) / *2*) ∧ (*p* >(*sqrt*(*4*∗*l*+*1*) − *1*) / *2*)
proof−
have *p^2* − *p*∗(*sqrt*(*4*∗*l*+*1*))+ *l* +*1*/*4* < *1*/*4*
using ‹*p^2* − *p*∗(*sqrt*(*4*∗*l*+*1*))+ *l*<*0*› **by** *simp*
moreover

have $-\ (2*(p*\ sqrt(4*l\ +1))/2)\ +\ (4*\ l\ +1)/4\ =\ -\ p*(sqrt(4*l+1))+\ l\ +1/4$
by *force*
ultimately have $***$: $p\hat{}2\ -\ (2*(p*\ sqrt(4*l\ +1))/2)\ +\ (4*\ l\ +1)/4\ \ <1/4$
by *linarith*
have $****$: $(p\ -(sqrt(4*l\ +1))/2)\hat{}2\ =\ p\hat{}2\ -2\ *\ p*\ (sqrt(4*l\ +1))/2+\ ((sqrt(4*l\ +1))/2)\hat{}2$
by (*simp add*: *power2-diff*)
then have $p\hat{}2\ -2\ *\ p*\ (sqrt(4*l+1))/2+\ ((sqrt(4*l\ +1))/2)\hat{}2\ =\ p\hat{}2\ -2\ *\ p*\ (sqrt(4*l\ +1))/2+\ (4*l\ +1)/4$
by (*smt* (*verit*) *assms*(*1*) *power-divide real-sqrt-four real-sqrt-pow2*)
then have $(p\ -(sqrt(4*l\ +1))/2)\hat{}2\ <1/4$ **using** $***$ $****$ **by** *linarith*
then have $|(p\ -(sqrt(4*l\ +1))/2)\ |\ <1/2$
by (*metis real-sqrt-abs real-sqrt-divide real-sqrt-four real-sqrt-less-mono real-sqrt-one*)
then have $((p\ -(sqrt(4*l\ +1))/2)\ )\ <1/2\ \ ((p\ -(sqrt(4*l\ +1))/2)\ )\ >\ -1/2$ **by** *linarith+*
then show *?thesis*
by *force*
qed

So p lies in an interval of length strictly less than 1 between two positive integers, but this means that p cannot be a positive integer, which yields the desired contradiction, thus completing the proof:

obtain *A*::*nat* **where** *A*: $real\ A\ =\ -\ 1/2\ +\ (1/2)*\ sqrt(4*l\ +1)$
using *ru* **by** *blast*
then show *False*
using *4 p* **by** *fastforce*
qed
qed

Finally, for convenience and completeness, we state the special case where equality holds formulated with the double implication and moreover including the values for which the INF (i.e. minimum here as we have seen) is attained as previously calculated.

theorem *elementary-discrete-ineq-Wooley-special-case-iff*:
fixes *l*::*real* **and** *g*::*nat* $\Rightarrow$ *real*
assumes $l>0$ **and** $R=\{r::nat.\ r>0\}$ **and** $\forall\ r.\ g\ r\ =\ r+\ (l/r)$
shows $((INF\ r\in R.\ g\ r)\ =\ sqrt(4*l+1))\longleftrightarrow(\exists\ m::nat.\ l\ =m*(m-1))$
and
$g\ p\ =sqrt(4*l+1)\ \longrightarrow\ (p\ =\ 1/2\ +\ (1/2)*\ sqrt(\ 4*l\ +1))\ \vee\ (p\ =\ -1/2\ +\ (1/2)*\ sqrt(4*l\ +1))$
using *assms elementary-discrete-ineq-Wooley-special-case-1 elementary-discrete-ineq-Wooley-special-case-2*
apply *blast*
using *assms*(*1*) *assms*(*3*) *elementary-discrete-ineq-Wooley-quadratic-eq-sol restrict-to-min*
by *auto*

end

References

[1] T. D. Wooley. An elementary discrete inequality. https://www.math.purdue.edu/~twooley/publ/20230410discineq.pdf.