Problem 96 with PVS

Kai Engelhardt

April 1, 2023

Problem number *96. Principle of Inclusion/Exclusion* from the list of the "top 100" of mathematical theorems didn't have a PVS formalisation and proof yet.

We prove said *inclusion-exclusion principle*, that is:

$$\left|\bigcup S\right| = \sum_{\emptyset\neq T\subseteq S} (-1)^{|T|+1}\left|\bigcap T\right|$$

for all finite sets S of finite sets. The proof attempts to follow that of Lehman et al. [2018, p. 718f]. Cryptic lemma names such as `e15_16` recall their equation numbering.

1 A PVS Encoding

1.1 `real_aux.pvs`

```
real_aux[D: TYPE+]: THEORY
% EXPORTING e15_16 WITH CLOSURE
BEGIN
ASSUMING
  % not sure this is a good idea
  finite_universe: ASSUMPTION is_finite_type[D]
ENDASSUMING

IMPORTING finite_sets@finite_sets_product_real[D]
% IMPORTING finite_sets@finite_sets_sum_real[finite_set[D]]
IMPORTING powerset_aux[D]
IMPORTING finite_sum_aux[set[D],set[D]] % should the 2nd be non_empty_finite_set[D]?
IMPORTING finite_sum_aux2[set[D]]
IMPORTING weak_ext2 % '2' for second attempt


A,B: VAR finite_set[D]
f: VAR [D -> real]
x: VAR D

n_f(f)(x): real = 1 - f(x)

% proof step lemmas, hardly useful outside
e15_16_1: LEMMA
  nonempty?(A) =>
  product(A,n_f(f)) = n_f(f)(choose(A)) * product(rest(A),n_f(f))

e15_16_2: LEMMA
  nonempty?(A) =>
    f(choose(A)) * sum(powerset(rest(A)), lambda B: (-1)^(card(B)) * product(B,f))
  = sum(powerset(rest(A)), lambda B: (-1)^(card(B)) * f(choose(A)) * product(B,f))
```

```
e15_16_3: LEMMA
  nonempty?(A) =>
  - sum(powerset(rest(A)), lambda B: (-1)^(card(B)) * f(choose(A)) * product(B,f))
  = sum(powerset(rest(A)), lambda B: (-1)^(card(B)+1) * f(choose(A)) * product(B,f))

e15_16_4: LEMMA
  nonempty?(A) =>
    sum(powerset(rest(A)), lambda B: (-1)^(card(B)+1) * f(choose(A)) * product(B,f))
  = sum(powerset(rest(A)), (lambda B: (-1)^(card(B)) * product(B,f)) o (lambda B: add(choose(A),B)))

% e15_16_5: LEMMA
%   nonempty?(A) =>
%     sum(powerset(rest(A)), (lambda B: (-1)^(card(B)) * product(B,f)) o (lambda B: add(choose(A),B)))
%   = sum(image(lambda B: add(choose(A),B), powerset(rest(A))),
%          (lambda B: (-1)^(card(B)) * product(B,f)))

e15_16_6: LEMMA
  nonempty?(A) =>
    sum(powerset(rest(A)), lambda B: (-1)^(card(B)) * product(B,f))
  + sum(image(lambda B: add(choose(A),B), powerset(rest(A))),
        lambda B: (-1)^(card(B)) * product(B,f))
  = sum(powerset(A)      , lambda B: (-1)^(card(B)) * product(B,f))

% somewhat useful
e15_16: LEMMA
  product(A,n_f(f)) =
  sum(powerset(A), lambda B: (-1)^(card(B)) * product(B,f))

END real_aux
```

1.2 powerset_aux.pvs

```
powerset_aux[T: TYPE+]: THEORY
BEGIN
A: VAR (nonempty?[T])
G: VAR set[T]
F: VAR non_empty_finite_set[T]
B: VAR finite_set[T]


disjoint_choose_rest: LEMMA
  disjoint?(singleton(choose(A)), rest(A))

union_choose_rest: LEMMA
  union(singleton(choose(A)), rest(A)) = A

add_choose_rest: LEMMA
  add(choose(A), rest(A)) = A

powerset_finite2: JUDGEMENT
    powerset(B) HAS_TYPE finite_set[finite_set[T]]

powerset_finite3: JUDGEMENT
    powerset(B) HAS_TYPE non_empty_finite_set[finite_set[T]]

powerset_im_add_c2pr_disjoint : LEMMA
  disjoint?(powerset(rest(A)), image(lambda G: add(choose(A),G), powerset(rest(A))))

powerset_rew: LEMMA
  union(powerset(rest(A)), image(lambda G: add(choose(A),G), powerset(rest(A)))) = powerset(A)

nv_sub_ss(G): set[set[T]] =
  { A | subset?(A,G) }
```

```
nv_sub_ss_powerset: LEMMA
  remove(emptyset, powerset(A)) = nv_sub_ss(A)

% nv_sub_ss_finite: JUDGEMENT
%   nv_sub_ss(B) HAS_TYPE finite_set[finite_set[T]]

nv_sub_ss_rest: LEMMA
  union(nv_sub_ss(rest(A)), image(lambda G: add(choose(A),G), powerset(rest(A)))) = nv_sub_ss(A)

END powerset_aux
```

1.3 weak_ext2.pvs

```
weak_ext2[T: TYPE+, A: TYPE FROM T, B: TYPE FROM T]: THEORY
BEGIN
P: VAR pred[T]
a: VAR A
b: VAR B
x: VAR T

weak_ext_half: LEMMA
  % (FORALL x: A_pred(x) AND P(x) => B_pred(x)) =>
  % subset?({a | P(a)}, {b | P(b)})
  (FORALL a: P(a) => B_pred(a)) =>
  subset?({x | A_pred(x) AND P(x)}, {x | B_pred(x) AND P(x)})

weak_ext: LEMMA
  % (FORALL x: A_pred(x) AND P(x) => B_pred(x)) =>
  % (FORALL x: B_pred(x) AND P(x) => A_pred(x)) =>
  % {b | P(b)} = {a | P(a)}
  (FORALL a: P(a) => B_pred(a)) AND (FORALL b: P(b) => A_pred(b)) =>
  {x | A_pred(x) AND P(x)} = {x | B_pred(x) AND P(x)}

% Can't have this:
%
% weak_ext2: LEMMA
%   % (FORALL x: A_pred(x) AND P(x) => B_pred(x)) =>
%   % (FORALL x: B_pred(x) AND P(x) => A_pred(x)) =>
%   % {b | P(b)} = {a | P(a)}
%   (FORALL a: P(a) => B_pred(a)) AND (FORALL b: P(b) => A_pred(b)) =>
%   {x: A | P(x)} = {x: B | P(x)}
%
% because it generates an unprovable TCC:
%
% % Subtype TCC generated (at line 26, column 18) for  {x: B | P(x)}
%     % expected type  [A -> bool]
%   % unfinished
% weak_ext2_TCC1: OBLIGATION
%   FORALL (P: pred[T]):
%     ((FORALL b: P(b) => A_pred(b)) AND FORALL a: P(a) => B_pred(a)) IMPLIES
%      FORALL (x1: T): B_pred(x1) IFF A_pred(x1);

set_comprehension_shift_type: LEMMA
  {x | A_pred(x) AND P(x)} = {a | P(a)}


END weak_ext2
```

1.4 finite_sum_aux.pvs

```
finite_sum_aux[D1, D2: TYPE+]: THEORY
BEGIN
IMPORTING finite_sets@finite_sets_sum_real[D1]
IMPORTING finite_sets@finite_sets_sum_real[D2]
```

```
X: VAR finite_set[D1]
x: VAR D1
Y: VAR finite_set[D2]
y: VAR D2
g: VAR [D1 -> D2]
f: VAR [D2 -> real]
h: VAR [D1 -> [D2 -> real]]

sum_map_dom: LEMMA
  injective?[(X), (image(g,X))](g) =>
  sum(X, f o g) = sum(image(g,X), f)

sum_swap: LEMMA
  sum(X,lambda x: sum(Y, h(x))) = sum(Y, lambda y: sum(X, lambda x: h(x)(y)))

END finite_sum_aux

finite_sum_aux2[D: TYPE+]: THEORY
BEGIN
IMPORTING finite_sets@finite_sets_sum_real[D]

A,B: VAR finite_set[D]
f,g: VAR [D -> real]
x: VAR D

sum_distributive2: THEOREM
  sum(A,f) - sum(A,g) = sum(A,(LAMBDA x: f(x) - g(x)))

sum_eq_doms: LEMMA
  A = B => sum(A,f) = sum(B,f)
END finite_sum_aux2
```

1.5 M_D_aux.pvs

```
M_D_aux[T: TYPE+]: THEORY

BEGIN
IMPORTING finite_sets@finite_sets_sum_real[T]
IMPORTING finite_sets@finite_sets_product_real[finite_set[T]]

a,b: VAR set[T]
D: VAR finite_set[T]
A,B,C: VAR finite_set[finite_set[T]]
c,n: VAR nat
x: VAR T

M_D(a): [T -> nbit] =
  b2n o a

neg_M_D(a): [T -> nbit] =
  b2n o (NOT) o a

neg_is_minus: LEMMA
  neg_M_D(a)(x) = 1 - M_D(a)(x)

union_dual: LEMMA
  M_D(union(a,b))(x) = 1 - neg_M_D(a)(x) * neg_M_D(b)(x)

intersection_is_product: LEMMA
  M_D(intersection(a,b))(x) = M_D(a)(x) * M_D(b)(x)

M_D_sum: LEMMA
  subset?(a,D) => card(a) = sum(D,M_D(a))

```

```
union_dual3: LEMMA
  M_D(Union(A))(x) = 1 - product(A,lambda a:neg_M_D(a)(x))

intersection_is_product3: LEMMA
  M_D(Intersection(A))(x) = product(A,lambda a:M_D(a)(x))

END M_D_aux
```

1.6 p96.pvs

```
p96[T: TYPE+]: THEORY
BEGIN
ASSUMING
  % not sure this is a good idea
  finite_universe: ASSUMPTION is_finite_type[T]
ENDASSUMING

IMPORTING finite_sets@finite_sets_sum_real[T]
IMPORTING finite_sets@finite_sets_sum[finite_set[finite_set[T]],real,0,+] AS FFS
IMPORTING finite_sets@card_tricks
IMPORTING powerset_aux[T]
IMPORTING real_aux[finite_set[T]]
IMPORTING finite_sum_aux[T,finite_set[finite_set[T]]]
IMPORTING finite_sum_aux2[T]
IMPORTING finite_sum_aux2[finite_set[T]]
IMPORTING M_D_aux[T]

a,b: VAR finite_set[T]
D: VAR non_empty_finite_set[T]
A,B,C: VAR finite_set[finite_set[T]]
c,n: VAR nat
x: VAR T

altcard(B): int =
  (-1)^(card(B) + 1) * card(Intersection(B))

% lemmas for the steps, mostly to find type problems
e15_22_1: LEMMA
  (FORALL (a: (A)): subset?(a, D)) IMPLIES
  card(Union(A)) = sum(D,M_D(Union(A)))

e15_22_2: LEMMA
  (FORALL (a: (A)): subset?(a, D)) IMPLIES
  sum(D,M_D(Union(A))) = sum(D,lambda x: 1 - product(A,lambda a:neg_M_D(a)(x)))

e15_22_3: LEMMA
  (FORALL (a: (A)): subset?(a, D)) AND D(x) IMPLIES
    product(A,lambda a:neg_M_D(a)(x))
  = FFS.sum(powerset(A), lambda B: (-1)^(card(B)) * product(B, lambda a: M_D(a)(x)))

e15_22_3b: LEMMA
  (FORALL (a: (A)): subset?(a, D)) AND D(x) IMPLIES
    FFS.sum(powerset(A), lambda B: (-1)^(card(B)) * product(B, lambda a: M_D(a)(x)))
  = FFS.sum(powerset(A), lambda B: (-1)^(card(B)) * M_D(Intersection(B))(x))

e15_22_4: LEMMA
  (FORALL (a: (A)): subset?(a, D)) IMPLIES
    sum(D,lambda x: 1 - FFS.sum(powerset(A), lambda B: (-1)^(card(B)) * M_D(Intersection(B))(x)))
  = card(D) - sum(D,lambda x: FFS.sum(powerset(A), lambda B: (-1)^(card(B)) * M_D(Intersection(B))(x)))

e15_22_5: LEMMA
  (FORALL (a: (A)): subset?(a, D)) IMPLIES
    sum(D,lambda x: FFS.sum(powerset(A), lambda B: (-1)^(card(B)) * M_D(Intersection(B))(x)))
  = sum(D,lambda x: FFS.sum(remove(emptyset,powerset(A)), lambda B: (-1)^(card(B)) * M_D(Intersection(B))(x)))
  + sum(D,lambda x: sum(singleton(emptyset), lambda B: (-1)^(card(B)) * M_D(Intersection(B))(x)))
```

```
e15_22_6a: LEMMA
  (FORALL (a: (A)): subset?(a, D)) IMPLIES
    sum(D,lambda x: FFS.sum(remove(emptyset,powerset(A)), lambda B: (-1)^(card(B)) * M_D(Intersection(B))(x)))
  = FFS.sum(remove(emptyset,powerset(A)), lambda B: (-1)^(card(B)) * sum(D,lambda x: M_D(Intersection(B))(x)))

e15_22_6b: LEMMA
  (FORALL (a: (A)): subset?(a, D)) IMPLIES
    sum(D,lambda x: sum(singleton(emptyset), lambda B: (-1)^(card(B)) * M_D(Intersection(B))(x)))
  = card(D)

e15_22_7: LEMMA
  (FORALL (a: (A)): subset?(a, D)) IMPLIES
    sum(D,lambda x: 1 - FFS.sum(powerset(A), lambda B: (-1)^(card(B)) * M_D(Intersection(B))(x)))
  = FFS.sum(remove(emptyset,powerset(A)), lambda B: (-1)^(card(B) + 1) * sum(D,lambda x: M_D(Intersection(B))(x)))


% 15.22 problem 96
inclusion_exclusion: THEOREM
  (FORALL (a: (A)): subset?(a, D)) IMPLIES
  card(Union(A)) = FFS.sum(remove(emptyset,powerset(A)), altcard)

END p96
```

1.7 Proof Status

```
Proof summary for theory real_aux
   e15_16_1..............................proved - complete   [SHOSTAK](0.00 s)
   e15_16_2_TCC1.........................proved - complete   [SHOSTAK](0.00 s)
   e15_16_2..............................proved - complete   [SHOSTAK](0.00 s)
   e15_16_3..............................proved - complete   [SHOSTAK](0.00 s)
   e15_16_4..............................proved - complete   [SHOSTAK](0.00 s)
   e15_16_6..............................proved - complete   [SHOSTAK](0.00 s)
   e15_16_TCC1...........................proved - complete   [SHOSTAK](0.00 s)
   e15_16................................proved - complete   [SHOSTAK](0.00 s)
   Theory real_aux totals: 8 formulas, 8 attempted, 8 succeeded (0.01 s)

Proof summary for theory powerset_aux
   disjoint_choose_rest..................proved - complete   [SHOSTAK](0.00 s)
   union_choose_rest.....................proved - complete   [SHOSTAK](0.00 s)
   add_choose_rest.......................proved - complete   [SHOSTAK](0.00 s)
   powerset_finite3......................proved - complete   [SHOSTAK](0.00 s)
   powerset_im_add_c2pr_disjoint.........proved - complete   [SHOSTAK](0.00 s)
   powerset_rew..........................proved - complete   [SHOSTAK](0.00 s)
   nv_sub_ss_powerset....................proved - complete   [SHOSTAK](0.00 s)
   nv_sub_ss_rest........................proved - complete   [SHOSTAK](0.00 s)
   Theory powerset_aux totals: 8 formulas, 8 attempted, 8 succeeded (0.00 s)

Proof summary for theory weak_ext2
   weak_ext_half.........................proved - complete   [SHOSTAK](0.00 s)
   weak_ext..............................proved - complete   [SHOSTAK](0.00 s)
   set_comprehension_shift_type..........proved - complete   [SHOSTAK](0.00 s)
   Theory weak_ext2 totals: 3 formulas, 3 attempted, 3 succeeded (0.00 s)

Proof summary for theory finite_sum_aux
   sum_map_dom_TCC1......................proved - complete   [SHOSTAK](0.00 s)
   sum_map_dom...........................proved - complete   [SHOSTAK](0.00 s)
```

```
    sum_swap............................proved - complete   [SHOSTAK](0.00 s)
    Theory finite_sum_aux totals: 3 formulas, 3 attempted, 3 succeeded (0.00 s)

 Proof summary for theory finite_sum_aux2
    sum_distributive2...................proved - complete   [SHOSTAK](0.00 s)
    sum_eq_doms.........................proved - complete   [SHOSTAK](0.00 s)
    Theory finite_sum_aux2 totals: 2 formulas, 2 attempted, 2 succeeded (0.00 s)

 Proof summary for theory M_D_aux
    neg_is_minus........................proved - complete   [SHOSTAK](0.00 s)
    union_dual..........................proved - complete   [SHOSTAK](0.00 s)
    intersection_is_product.............proved - complete   [SHOSTAK](0.00 s)
    M_D_sum_TCC1........................proved - complete   [SHOSTAK](0.00 s)
    M_D_sum.............................proved - complete   [SHOSTAK](0.00 s)
    union_dual3.........................proved - complete   [SHOSTAK](0.00 s)
    intersection_is_product3............proved - complete   [SHOSTAK](0.00 s)
    Theory M_D_aux totals: 7 formulas, 7 attempted, 7 succeeded (0.00 s)

 Proof summary for theory p96
    FFS_TCC1............................proved - complete   [SHOSTAK](0.00 s)
    FFS_TCC2............................proved - complete   [SHOSTAK](0.00 s)
    IMP_real_aux_TCC1...................proved - complete   [SHOSTAK](0.00 s)
    altcard_TCC1........................proved - complete   [SHOSTAK](0.00 s)
    e15_22_1_TCC1.......................proved - complete   [SHOSTAK](0.00 s)
    e15_22_1............................proved - complete   [SHOSTAK](0.00 s)
    e15_22_2............................proved - complete   [SHOSTAK](0.00 s)
    e15_22_3............................proved - complete   [SHOSTAK](0.00 s)
    e15_22_3b...........................proved - complete   [SHOSTAK](0.00 s)
    e15_22_4............................proved - complete   [SHOSTAK](0.00 s)
    e15_22_5............................proved - complete   [SHOSTAK](0.00 s)
    e15_22_6a...........................proved - complete   [SHOSTAK](0.00 s)
    e15_22_6b...........................proved - complete   [SHOSTAK](0.00 s)
    e15_22_7............................proved - complete   [SHOSTAK](0.00 s)
    inclusion_exclusion.................proved - complete   [SHOSTAK](0.00 s)
    Theory p96 totals: 15 formulas, 15 attempted, 15 succeeded (0.01 s)

Grand Totals: 46 proofs, 46 attempted, 46 succeeded (0.02 s)
```

NB: those times are bogus.

References

Eric Lehman, F. Thomson Leighton, and Albert R. Meyer. Mathematics for computer science. Available at https://courses.csail.mit.edu/6.042/spring18/mcs.pdf; check https://courses.csail.mit.edu/6.042 for newer versions, 2018.