

Problem 96 with PVS

Kai Engelhardt

March 28, 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`

```
1  real_aux[D: TYPE+]: THEORY
2  % EXPORTING e15_16 WITH CLOSURE
3  BEGIN
4  ASSUMING
5    % not sure this is a good idea
6    finite_universe: ASSUMPTION is_finite_type[D]
7  ENDASSUMING
8
9  IMPORTING finite_sets@finite_sets_product_real[D]
10 % IMPORTING finite_sets@finite_sets_sum_real[finite_set[D]]
11 IMPORTING powerset_aux[D]
12 IMPORTING finite_sum_aux[set[D],set[D]] % should the 2nd be non_empty_finite_set[D]?
13 IMPORTING finite_sum_aux2[set[D]]
14 IMPORTING weak_ext2 % '2' for second attempt
15
16
17 A,B: VAR finite_set[D]
18 f: VAR [D -> real]
19 x: VAR D
20
21 n_f(f)(x): real = 1 - f(x)
22
23 % proof step lemmas, hardly useful outside
24 e15_16_1: LEMMA
25   nonempty?(A) =>
26     product(A,n_f(f)) = n_f(f)(choose(A)) * product(rest(A),n_f(f))
27
28 e15_16_2: LEMMA
29   nonempty?(A) =>
30     f(choose(A)) * sum(powerset(rest(A)), lambda B: (-1)^(card(B)) * product(B,f))
31   = sum(powerset(rest(A)), lambda B: (-1)^(card(B)) * f(choose(A)) * product(B,f))
```

```

32
33 e15_16_3: LEMMA
34   nonempty?(A) =>
35   - sum(powerset(rest(A)), lambda B: (-1)^(card(B)) * f(choose(A)) * product(B,f))
36   = sum(powerset(rest(A)), lambda B: (-1)^(card(B)+1) * f(choose(A)) * product(B,f))
37
38 e15_16_4: LEMMA
39   nonempty?(A) =>
40     sum(powerset(rest(A)), lambda B: (-1)^(card(B)+1) * f(choose(A)) * product(B,f))
41   = sum(powerset(rest(A)), (lambda B: (-1)^(card(B)) * product(B,f)) o (lambda B: add(choose(A),B)))
42
43 % e15_16_5: LEMMA
44 %   nonempty?(A) =>
45 %     sum(powerset(rest(A)), (lambda B: (-1)^(card(B)) * product(B,f)) o (lambda B: add(choose(A),B)))
46 %   = sum(image(lambda B: add(choose(A),B), powerset(rest(A))),
47 %     (lambda B: (-1)^(card(B)) * product(B,f)))
48
49 e15_16_6: LEMMA
50   nonempty?(A) =>
51     sum(powerset(rest(A)), lambda B: (-1)^(card(B)) * product(B,f))
52   + sum(image(lambda B: add(choose(A),B), powerset(rest(A))),
53     lambda B: (-1)^(card(B)) * product(B,f))
54   = sum(powerset(A), lambda B: (-1)^(card(B)) * product(B,f))
55
56 % somewhat useful
57 e15_16: LEMMA
58   product(A,n_f(f)) =
59   sum(powerset(A), lambda B: (-1)^(card(B)) * product(B,f))
60
61 END real_aux

```

1.2 powerset_aux.pvs

```

1 powerset_aux[T: TYPE+]: THEORY
2 BEGIN
3 A: VAR (nonempty?[T])
4 G: VAR set[T]
5 F: VAR non_empty_finite_set[T]
6 B: VAR finite_set[T]
7
8
9 disjoint_choose_rest: LEMMA
10   disjoint?(singleton(choose(A)), rest(A))
11
12 union_choose_rest: LEMMA
13   union(singleton(choose(A)), rest(A)) = A
14
15 add_choose_rest: LEMMA
16   add(choose(A), rest(A)) = A
17
18 powerset_finite2: JUDGEMENT
19   powerset(B) HAS_TYPE finite_set[finite_set[T]]
20
21 powerset_finite3: JUDGEMENT
22   powerset(B) HAS_TYPE non_empty_finite_set[finite_set[T]]
23
24 powerset_im_add_c2pr_disjoint : LEMMA
25   disjoint?(powerset(rest(A)), image(lambda G: add(choose(A),G), powerset(rest(A))))
26
27 powerset_rew: LEMMA
28   union(powerset(rest(A)), image(lambda G: add(choose(A),G), powerset(rest(A)))) = powerset(A)
29
30 nv_sub_ss(G): set[set[T]] =
31   { A | subset?(A,G) }
32

```

```

33 nv_sub_ss_powerset: LEMMA
34   remove(emptyset, powerset(A)) = nv_sub_ss(A)
35
36 % nv_sub_ss_finite: JUDGEMENT
37 %   nv_sub_ss(B) HAS_TYPE finite_set[finite_set[T]]
38
39 nv_sub_ss_rest: LEMMA
40   union(nv_sub_ss(rest(A)), image(lambda G: add(choose(A),G), powerset(rest(A)))) = nv_sub_ss(A)
41
42 END powerset_aux

```

1.3 weak_ext2.pvs

```

1 weak_ext2[T: TYPE+, A: TYPE FROM T, B: TYPE FROM T]: THEORY
2 BEGIN
3 P: VAR pred[T]
4 a: VAR A
5 b: VAR B
6 x: VAR T
7
8 weak_ext_half: LEMMA
9   % (FORALL x: A_pred(x) AND P(x) => B_pred(x)) =>
10   % subset?({a | P(a)}, {b | P(b)})
11   (FORALL a: P(a) => B_pred(a)) =>
12   subset?({x | A_pred(x) AND P(x)}, {x | B_pred(x) AND P(x)})
13
14 weak_ext: LEMMA
15   % (FORALL x: A_pred(x) AND P(x) => B_pred(x)) =>
16   % (FORALL x: B_pred(x) AND P(x) => A_pred(x)) =>
17   % {b | P(b)} = {a | P(a)}
18   (FORALL a: P(a) => B_pred(a)) AND (FORALL b: P(b) => A_pred(b)) =>
19   {x | A_pred(x) AND P(x)} = {x | B_pred(x) AND P(x)}
20
21 % Can't have this:
22 %
23 % weak_ext2: LEMMA
24 %   % (FORALL x: A_pred(x) AND P(x) => B_pred(x)) =>
25 %   % (FORALL x: B_pred(x) AND P(x) => A_pred(x)) =>
26 %   % {b | P(b)} = {a | P(a)}
27 %   (FORALL a: P(a) => B_pred(a)) AND (FORALL b: P(b) => A_pred(b)) =>
28 %   {x: A | P(x)} = {x: B | P(x)}
29 %
30 % because it generates an unprovable TCC:
31 %
32 % % Subtype TCC generated (at line 26, column 18) for {x: B | P(x)}
33 %   % expected type [A -> bool]
34 %   % unfinished
35 % weak_ext2_TCC1: OBLIGATION
36 %   FORALL (P: pred[T]):
37 %     ((FORALL b: P(b) => A_pred(b)) AND FORALL a: P(a) => B_pred(a)) IMPLIES
38 %     FORALL (x1: T): B_pred(x1) IFF A_pred(x1);
39
40 set_comprehension_shift_type: LEMMA
41   {x | A_pred(x) AND P(x)} = {a | P(a)}
42
43
44 END weak_ext2

```

1.4 finite_sum_aux.pvs

```

1 finite_sum_aux[D1, D2: TYPE+]: THEORY
2 BEGIN
3 IMPORTING finite_sets@finite_sets_sum_real[D1]
4 IMPORTING finite_sets@finite_sets_sum_real[D2]

```

```

5
6 X: VAR finite_set[D1]
7 x: VAR D1
8 Y: VAR finite_set[D2]
9 y: VAR D2
10 g: VAR [D1 -> D2]
11 f: VAR [D2 -> real]
12 h: VAR [D1 -> [D2 -> real]]
13
14 sum_map_dom: LEMMA
15   injective?[(X), (image(g,X))](g) =>
16     sum(X, f o g) = sum(image(g,X), f)
17
18 sum_swap: LEMMA
19   sum(X, lambda x: sum(Y, h(x))) = sum(Y, lambda y: sum(X, lambda x: h(x)(y)))
20
21 END finite_sum_aux
22
23 finite_sum_aux2[D: TYPE+]: THEORY
24 BEGIN
25   IMPORTING finite_sets@finite_sets_sum_real[D]
26
27 A,B: VAR finite_set[D]
28 f,g: VAR [D -> real]
29 x: VAR D
30
31 sum_distributive2: THEOREM
32   sum(A,f) - sum(A,g) = sum(A, (LAMBDA x: f(x) - g(x)))
33
34 sum_eq_doms: LEMMA
35   A = B => sum(A,f) = sum(B,f)
36 END finite_sum_aux2

```

1.5 M_D_aux.pvs

```

1 M_D_aux[T: TYPE+]: THEORY
2
3 BEGIN
4   IMPORTING finite_sets@finite_sets_sum_real[T]
5   IMPORTING finite_sets@finite_sets_product_real[finite_set[T]]
6
7 a,b: VAR set[T]
8 D: VAR finite_set[T]
9 A,B,C: VAR finite_set[finite_set[T]]
10 c,n: VAR nat
11 x: VAR T
12
13 M_D(a): [T -> nbit] =
14   b2n o a
15
16 neg_M_D(a): [T -> nbit] =
17   b2n o (NOT) o a
18
19 neg_is_minus: LEMMA
20   neg_M_D(a)(x) = 1 - M_D(a)(x)
21
22 union_dual: LEMMA
23   M_D(union(a,b))(x) = 1 - neg_M_D(a)(x) * neg_M_D(b)(x)
24
25 intersection_is_product: LEMMA
26   M_D(intersection(a,b))(x) = M_D(a)(x) * M_D(b)(x)
27
28 M_D_sum: LEMMA
29   subset?(a,D) => card(a) = sum(D, M_D(a))
30

```

```

31 union_dual3: LEMMA
32   M_D(Union(A))(x) = 1 - product(A, lambda a: neg_M_D(a)(x))
33
34 intersection_is_product3: LEMMA
35   M_D(Intersection(A))(x) = product(A, lambda a: M_D(a)(x))
36
37 END M_D_aux

```

1.6 p96.pvs

```

1  p96[T: TYPE+]: THEORY
2  BEGIN
3  ASSUMING
4    % not sure this is a good idea
5    finite_universe: ASSUMPTION is_finite_type[T]
6  ENDASSUMING
7
8  IMPORTING finite_sets@finite_sets_sum_real[T]
9  IMPORTING finite_sets@finite_sets_sum[finite_set[finite_set[T]],real,0,+] AS FFS
10 IMPORTING finite_sets@card_tricks
11 IMPORTING real_aux[finite_set[T]]
12 IMPORTING finite_sum_aux[T,finite_set[finite_set[T]]]
13 IMPORTING finite_sum_aux2[T]
14 IMPORTING finite_sum_aux2[finite_set[T]]
15 IMPORTING M_D_aux[T]
16
17 a,b: VAR finite_set[T]
18 D: VAR non_empty_finite_set[T]
19 A,B,C: VAR finite_set[finite_set[T]]
20 c,n: VAR nat
21 x: VAR T
22
23 altcard(B): int =
24   (-1)^(card(B) + 1) * card(Intersection(B))
25
26 % lemmas for the steps, mostly to find type problems
27 e15_22_1: LEMMA
28   (FORALL (a: (A)): subset?(a, D)) IMPLIES
29   card(Union(A)) = sum(D, M_D(Union(A)))
30
31 e15_22_2: LEMMA
32   (FORALL (a: (A)): subset?(a, D)) IMPLIES
33   sum(D, M_D(Union(A))) = sum(D, lambda x: 1 - product(A, lambda a: neg_M_D(a)(x)))
34
35 e15_22_3: LEMMA
36   (FORALL (a: (A)): subset?(a, D)) AND D(x) IMPLIES
37   product(A, lambda a: neg_M_D(a)(x))
38   = FFS.sum(powerset(A), lambda B: (-1)^(card(B)) * product(B, lambda a: M_D(a)(x)))
39
40 e15_22_3b: LEMMA
41   (FORALL (a: (A)): subset?(a, D)) AND D(x) IMPLIES
42   FFS.sum(powerset(A), lambda B: (-1)^(card(B)) * product(B, lambda a: M_D(a)(x)))
43   = FFS.sum(powerset(A), lambda B: (-1)^(card(B)) * M_D(Intersection(B))(x))
44
45 e15_22_4: LEMMA
46   (FORALL (a: (A)): subset?(a, D)) IMPLIES
47   sum(D, lambda x: 1 - FFS.sum(powerset(A), lambda B: (-1)^(card(B)) * M_D(Intersection(B))(x)))
48   = card(D) - sum(D, lambda x: FFS.sum(powerset(A), lambda B: (-1)^(card(B)) * M_D(Intersection(B))(x)))
49
50 e15_22_5: LEMMA
51   (FORALL (a: (A)): subset?(a, D)) IMPLIES
52   sum(D, lambda x: FFS.sum(powerset(A), lambda B: (-1)^(card(B)) * M_D(Intersection(B))(x)))
53   = sum(D, lambda x: FFS.sum(remove(emptyset, powerset(A)), lambda B: (-1)^(card(B)) * M_D(Intersection(B))(x)))
54   + sum(D, lambda x: sum(singleton(emptyset), lambda B: (-1)^(card(B)) * M_D(Intersection(B))(x)))
55

```

```

56 e15_22_6a: LEMMA
57   (FORALL (a: (A)): subset?(a, D)) IMPLIES
58     sum(D, lambda x: FFS.sum(remove(emptyset, powerset(A)), lambda B: (-1)^(card(B)) * M_D(Intersection(B))(x)))
59   = FFS.sum(remove(emptyset, powerset(A)), lambda B: (-1)^(card(B)) * sum(D, lambda x: M_D(Intersection(B))(x)))
60
61 e15_22_6b: LEMMA
62   (FORALL (a: (A)): subset?(a, D)) IMPLIES
63     sum(D, lambda x: sum(singleton(emptyset), lambda B: (-1)^(card(B)) * M_D(Intersection(B))(x)))
64   = card(D)
65
66 e15_22_7: LEMMA
67   (FORALL (a: (A)): subset?(a, D)) IMPLIES
68     sum(D, lambda x: 1 - FFS.sum(powerset(A), lambda B: (-1)^(card(B)) * M_D(Intersection(B))(x)))
69   = FFS.sum(remove(emptyset, powerset(A)), lambda B: (-1)^(card(B) + 1) * sum(D, lambda x: M_D(Intersection(B))(x)))
70
71
72 % 15.22 problem 96
73 inclusion_exclusion: THEOREM
74   (FORALL (a: (A)): subset?(a, D)) IMPLIES
75     card(Union(A)) = FFS.sum(remove(emptyset, powerset(A)), altcard)
76
77 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] (0.01 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 (0.03 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.