FORMALIZED MATHEMATICS
Volume 31, 2023, Pages 53–57
DOI: 10.2478/forma-2023-0005
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

On the Formalization of Gram-Schmidt Process for Orthonormalizing a Set of Vectors

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Summary. In this article, we formalize the Gram-Schmidt process in the Mizar system [2], [3] (compare another formalization using Isabelle/HOL proof assistant [1]). This process is one of the most famous methods for orthonormalizing a set of vectors. The method is named after Jørgen Pedersen Gram and Erhard Schmidt [4]. There are many applications of the Gram-Schmidt process in the field of computer science, e.g., error correcting codes or cryptology [8]. First, we prove some preliminary theorems about real unitary space. Next, we formalize the definition of the Gram-Schmidt process that finds orthonormal basis. We followed [5] in the formalization, continuing work developed in [7], [6].

MSC: 65F25 94A11 97H60 68V20

Keywords: Gram-Schmidt process; orthonormal basis; linear algebra

MML identifier: `RUSUB_6`, version: `8.1.12 5.74.1441`

1. Preliminaries

Let V be a non empty RLS structure, r be a finite sequence of elements of $\mathbb{R}$, and x be a finite sequence of elements of V. The functor $r \circ x$ yielding a finite sequence of elements of V is defined by

(Def. 1) $\operatorname{len} it = \operatorname{len} x$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} x$ holds $it(i) = r_{/i} \cdot (x_{/i})$.

Now we state the proposition:

(1) Let us consider a real linear space V, a subset A of V, a finite sequence x of elements of V, and a finite sequence r of elements of $\mathbb{R}$. Suppose $\operatorname{rng} x \subseteq A$ and $\operatorname{len} x = \operatorname{len} r$. Then $\sum(r \circ x) \in \operatorname{Lin}(A)$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence x of elements of V for every finite sequence r of elements of $\mathbb{R}$ such that $\$_1 = \operatorname{len} x$ and $\operatorname{rng} x \subseteq A$ and $\operatorname{len} x = \operatorname{len} r$ holds $\sum(r \circ x) \in \operatorname{Lin}(A)$. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. □

Let us consider a real linear space V and subsets A, B of V. Now we state the propositions:

(2) If $A \subseteq$ the carrier of $\operatorname{Lin}(B)$, then $\operatorname{Lin}(A)$ is a subspace of $\operatorname{Lin}(B)$.

(3) Suppose $A \subseteq$ the carrier of $\operatorname{Lin}(B)$ and $B \subseteq$ the carrier of $\operatorname{Lin}(A)$. Then $\operatorname{Lin}(A) = \operatorname{Lin}(B)$. The theorem is a consequence of (2).

Let V be a non empty unitary space structure, u be a point of V, and x be a finite sequence of elements of V. The functor $(u|x)$ yielding a finite sequence of elements of $\mathbb{R}$ is defined by

(Def. 2) $\operatorname{len} it = \operatorname{len} x$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} x$ holds $it(i) = (u|x_{/i})$.

Now we state the propositions:

(4) Let us consider a non empty unitary space structure V, a point u of V, a finite sequence x of elements of V, and a natural number i. Suppose $1 \leqslant i \leqslant \operatorname{len} x$. Then $((u|x) \circ x)(i) = (u|x_{/i}) \cdot (x_{/i})$.

(5) Let us consider a real unitary space V, a point u of V, and a finite sequence x of elements of V. Then $(u|\sum x) = \sum(u|x)$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence x of elements of V such that $\$_1 = \operatorname{len} x$ holds $(u|\sum x) = \sum(u|x)$. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. □

(6) Let us consider a real unitary space V, a point u of V, a natural number n, and a finite sequence x of elements of V. Suppose $1 \leqslant n \leqslant \operatorname{len} x$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} x$ and $n \neq i$ holds $(u|x_{/i}) = 0$. Then $(u|\sum x) = (u|x_{/n})$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence x of elements of V such that $\$_1 = \operatorname{len} x$ and $1 \leqslant n \leqslant \operatorname{len} x$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} x$ and $n \neq i$ holds $(u|x_{/i}) = 0$ holds $(u|\sum x) = (u|x_{/n})$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. □

Let us consider a real unitary space H. Now we state the propositions:

(7) There exists a function F from (the carrier of H) $\times$ (the carrier of H)* into (the carrier of H)* such that for every point x of H for every finite sequence e of elements of H, there exists a finite sequence F_2 of elements of H such that $F_2 = F(x, e)$ and $F_2 = (x|e) \circ e$.

PROOF: Set $C =$ the carrier of H. Define $\mathcal{R}[\text{object}, \text{object}, \text{object}] \equiv$ there exists a point x of H and there exists a finite sequence e of elements of C such that $\$_1 = x$ and $\$_2 = e$ and there exists a finite sequence F_2 of elements of C such that $F_2 = \$_3$ and $F_2 = (x|e) \circ e$. For every objects x, y such that $x \in C$ and $y \in C^*$ there exists an object z such that $z \in C^*$ and $\mathcal{R}[x, y, z]$. Consider F being a function from $C \times C^*$ into C^* such that for every objects z, y such that $z \in C$ and $y \in C^*$ holds $\mathcal{R}[z, y, F(z, y)]$. $\square$

(8) Every orthonormal family of H is linearly independent.

PROOF: For every linear combination l of G such that $\sum l = 0_H$ holds the support of $l = \emptyset$. $\square$

2. Gram-Schmidt Process

Let H be a real unitary space. The functor $\text{Seq}_{\text{Proj}}(H)$ yielding a function from (the carrier of H) $\times$ (the carrier of H)* into (the carrier of H)* is defined by

(Def. 3) for every point x of H and for every finite sequence e of elements of H, there exists a finite sequence F_2 of elements of H such that $F_2 = it(x, e)$ and $F_2 = (x|e) \circ e$.

Now we state the proposition:

(9) Let us consider a real unitary space H, and a finite sequence x of elements of H. Suppose x is one-to-one and $\operatorname{rng} x$ is linearly independent and $1 \leqslant \operatorname{len} x$. Then there exists a finite sequence e of elements of H such that

- (i) $\operatorname{len} x = \operatorname{len} e$, and
- (ii) $\operatorname{rng} e$ is an orthonormal family of H, and
- (iii) e is one-to-one, and
- (iv) $\operatorname{Lin}(\operatorname{rng} x) = \operatorname{Lin}(\operatorname{rng} e)$, and
- (v) $e_{/1} = \frac{1}{\|x_{/1}\|} \cdot (x_{/1})$, and
- (vi) for every natural number k such that $1 \leqslant k < \operatorname{len} x$ there exists a finite sequence g of elements of H such that $g = (\text{Seq}_{\text{Proj}}(H))(\langle x_{/1+k}, e{\restriction}k\rangle)$ and $e_{/k+1} = \frac{1}{\|x_{/1+k} - \sum g\|} \cdot (x_{/1+k} - \sum g)$, and
- (vii) for every natural number k such that $k \leqslant \operatorname{len} x$ holds $\operatorname{rng}(e{\restriction}k)$ is an orthonormal family of H and $e{\restriction}k$ is one-to-one and $\operatorname{Lin}(\operatorname{rng}(x{\restriction}k)) = \operatorname{Lin}(\operatorname{rng}(e{\restriction}k))$.

PROOF: Set C = the carrier of H. Reconsider $F_1 = \bigcup\{C^i$, where i is a natural number : $i \leqslant \operatorname{len} x\}$ as a non empty set. Set $F = \mathrm{Seq}_{\mathrm{Proj}}(H)$. Define $\mathcal{R}[\text{object}, \text{object}, \text{object}] \equiv$ there exists a C-valued finite sequence e and there exists a natural number n such that $e = \$_2$ and $n = \$_1$ and if $\operatorname{len} e < \operatorname{len} x$, then there exists a C-valued finite sequence g such that $g = F(\langle x_{/1+\operatorname{len} e}, e\rangle)$ and $\$_3 = e \frown \langle \frac{1}{\|x_{/1+\operatorname{len} e} - \sum g\|} \cdot (x_{/1+\operatorname{len} e} - \sum g)\rangle$. For every natural number n such that $1 \leqslant n < \operatorname{len} x$ for every element e of F_1, there exists an element f of F_1 such that $\mathcal{R}[n, e, f]$. Set $E_0 = \langle \frac{1}{\|x_{/1}\|} \cdot (x_{/1})\rangle$.

Consider E being a finite sequence of elements of F_1 such that $\operatorname{len} E = \operatorname{len} x$ and $E(1) = E_0$ or $\operatorname{len} x = 0$ and for every natural number n such that $1 \leqslant n < \operatorname{len} x$ holds $\mathcal{R}[n, E(n), E(n+1)]$. For every natural number k such that $k < \operatorname{len} x$ there exists a finite sequence e of elements of C such that $\operatorname{len} e = k + 1$ and $E(k+1) = e$. For every natural number k such that $1 \leqslant k < \operatorname{len} x$ there exist finite sequences f, g of elements of C such that $E(k) = f$ and $\operatorname{len} f = k$ and $g = F(\langle x_{/1+k}, f\rangle)$ and $E(k+1) = f \frown \langle \frac{1}{\|x_{/1+k} - \sum g\|} \cdot (x_{/1+k} - \sum g)\rangle$. Define $\mathcal{Q}[\text{natural number}, \text{object}, \text{object}] \equiv$ there exist finite sequences f, g of elements of C and there exists a point e_1 of H such that $E(\$_1) = f$ and $\operatorname{len} f = \$_1$ and $e_1 = \$_3$ and $g = F(\langle x_{/1+\$_1}, f\rangle)$ and $E(\$_1 + 1) = f \frown \langle e_1 \rangle$ and $e_1 = \frac{1}{\|x_{/1+\$_1} - \sum g\|} \cdot (x_{/1+\$_1} - \sum g)$. For every natural number k such that $1 \leqslant k < \operatorname{len} x$ for every element e of H, there exists an element h of H such that $\mathcal{Q}[k, e, h]$. Set $e_0 = \frac{1}{\|x_{/1}\|} \cdot (x_{/1})$.

Consider e being a finite sequence of elements of H such that $\operatorname{len} e = \operatorname{len} x$ and $e(1) = e_0$ or $\operatorname{len} x = 0$ and for every natural number n such that $1 \leqslant n < \operatorname{len} x$ holds $\mathcal{Q}[n, e(n), e(n+1)]$. For every natural number n such that $1 \leqslant n < \operatorname{len} x$ there exist finite sequences f, g of elements of C such that $E(n) = f$ and $\operatorname{len} f = n$ and $g = F(\langle x_{/1+n}, f\rangle)$ and $E(n+1) = f \frown \langle e_{/n+1} \rangle$ and $e_{/n+1} = \frac{1}{\|x_{/1+n} - \sum g\|} \cdot (x_{/1+n} - \sum g)$. For every natural number n such that $1 \leqslant n \leqslant \operatorname{len} x$ holds $E(n) = e \restriction n$. For every natural number k such that $1 \leqslant k < \operatorname{len} x$ there exists a finite sequence g of elements of C such that $g = F(\langle x_{/1+k}, e \restriction k\rangle)$ and $e_{/k+1} = \frac{1}{\|x_{/1+k} - \sum g\|} \cdot (x_{/1+k} - \sum g)$. Define $\mathcal{S}[\text{natural number}] \equiv$ if $\$_1 \leqslant \operatorname{len} x$, then $\operatorname{rng}(e \restriction \$_1)$ is an orthonormal family of H and $e \restriction \$_1$ is one-to-one and $\operatorname{Lin}(\operatorname{rng}(x \restriction \$_1)) = \operatorname{Lin}(\operatorname{rng}(e \restriction \$_1))$. $\mathcal{S}[0]$. For every natural number k such that $\mathcal{S}[k]$ holds $\mathcal{S}[k+1]$. For every natural number k, $\mathcal{S}[k]$. $\square$

Let H be a real unitary space and x be a finite sequence of elements of H. Assume x is one-to-one and $\operatorname{rng} x$ is linearly independent and $1 \leqslant \operatorname{len} x$. The functor $\mathrm{PROCESS}_{\mathrm{GramSchmidt}}(x)$ yielding a finite sequence of elements of H is defined by

(Def. 4) $\operatorname{len} x = \operatorname{len} it$ and $\operatorname{rng} it$ is an orthonormal family of H and it is one-to-one and $\operatorname{Lin}(\operatorname{rng} x) = \operatorname{Lin}(\operatorname{rng} it)$ and $it_{/1} = \frac{1}{\|x_{/1}\|} \cdot (x_{/1})$ and for every natural number k such that $1 \leqslant k < \operatorname{len} x$ there exists a finite sequence g of elements of H such that $g = (\mathrm{Seq}_{\mathrm{Proj}}(H))(\langle x_{/1+k}, it\restriction k\rangle)$ and $it_{/k+1} = \frac{1}{\|x_{/1+k} - \sum g\|} \cdot (x_{/1+k} - \sum g)$ and for every natural number k such that $k \leqslant \operatorname{len} x$ holds $\operatorname{rng}(it\restriction k)$ is an orthonormal family of H and $it\restriction k$ is one-to-one and $\operatorname{Lin}(\operatorname{rng}(x\restriction k)) = \operatorname{Lin}(\operatorname{rng}(it\restriction k))$.

Now we state the proposition:

(10) Let us consider a real unitary space H, and a finite sequence x of elements of H. Suppose x is one-to-one and $\operatorname{rng} x$ is linearly independent and $1 \leqslant \operatorname{len} x$. Then $\operatorname{rng} \mathrm{PROCESS}_{\mathrm{GramSchmidt}}(x)$ is linearly independent. The theorem is a consequence of (8).

Acknowledgement: The author would like to express his gratitude to Prof. Yasunari Shidama for his support and encouragement.

References

[1] Jesús Aransay and Jose Divasón. A formalisation in HOL of the fundamental theorem of linear algebra and its application to the solution of the least squares problem. *Journal of Automated Reasoning*, 58(4):509–535, 2017. doi:10.1007/s10817-016-9379-z.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[3] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[4] Ward Cheney and David Kincaid. *Linear Algebra: Theory and Applications.* Jones and Bartlett publishers, 2009.

[5] David G. Luenberger. *Optimization by Vector Space Methods.* John Wiley and Sons, 1969.

[6] Kazuhisa Nakasho, Hiroyuki Okazaki, and Yasunari Shidama. Real vector space and related notions. *Formalized Mathematics*, 29(**3**):117–127, 2021. doi:10.2478/forma-2021-0012.

[7] Hiroyuki Okazaki. Formalization of orthogonal decomposition for Hilbert spaces. *Formalized Mathematics*, 30(**4**):295–299, 2022. doi:10.2478/forma-2022-0023.

[8] René Thiemann and Akihisa Yamada. Formalizing Jordan Normal Forms in Isabelle/HOL. In *Proceedings of the 5th ACM SIGPLAN Conference on Certified Programs and Proofs*, pages 88–99, New York, NY, USA, 2016. Association for Computing Machinery. ISBN 9781450341271. doi:10.1145/2854065.2854073.

Accepted March 31, 2023