# A meet-in-the-middle algorithm for finding extremal restricted additive 2-bases 

Jukka Kohonen<br>Department of Mathematics and Statistics<br>P. O. Box 68<br>FI-00014 University of Helsinki<br>Finland<br>jukka.kohonen@helsinki.fi


#### Abstract

An additive 2-basis with range $n$ is restricted if its largest element is $n / 2$. Among the restricted 2 -bases of given length $k$, the ones that have the greatest range are extremal restricted. We describe an algorithm that finds the extremal restricted 2-bases of a given length, and we list them for lengths up to $k=41$.


## 1 Introduction

Let $n$ be a positive integer. An additive 2-basis for $n$, or more briefly a basis for $n$, is a set of integers $A_{k}=\left\{0=a_{0}<a_{1}<\cdots<a_{k}\right\}$ such that every integer in $[0, n]$ is the sum of two of its elements, not necessarily distinct. The length of the basis is $k$. The largest possible $n$ for a basis $A_{k}$ is its range and denoted $n_{2}\left(A_{k}\right)$. The maximum range among all bases of length $k$ is $n_{2}(k)$, and a basis that attains this maximum is extremal.

A basis $A_{k}$ is admissible if $n_{2}\left(A_{k}\right) \geq a_{k}$, restricted if $n_{2}\left(A_{k}\right) \geq 2 a_{k}$, and symmetric if $a_{i}+a_{k-i}=a_{k}$ for all $0 \leq i \leq k$. Since for any basis $n_{2}\left(A_{k}\right) \leq 2 a_{k}$, a restricted basis has in fact $n_{2}\left(A_{k}\right)=2 a_{k}$ exactly.

The maximum range among restricted bases is called the extremal restricted range and denoted $n_{2}^{*}(k)$, and an extremal restricted basis is one that attains this maximum. For many values of $k$, at least some of the extremal bases are restricted, so that $n_{2}^{*}(k)=n_{2}(k)$. This is not always true: a counterexample is $k=10$, where $n_{2}^{*}(10)=44$, but $n_{2}(10)=46$ (see Table 1).

Similarly, the maximum range among symmetric bases can be called the extremal symmetric range, and a basis that attains this maximum can be called extremal symmetric basis. Extremal symmetric bases are known up to $k=30$ due to Mossige [5].

All extremal bases of lengths $k \leq 24$ are currently known [3]. Interestingly, all of them are either both symmetric and restricted, or neither. Three questions arise naturally:

1. If an extremal basis is symmetric, is it necessarily restricted?

| range | notes | basis |
| :---: | :---: | :---: |
| 44 | R,A | $01237111517202122 \dagger$ |
| 44 | R,S | 01237111519202122 |
| 44 | R,S | 01257111517202122 |
| 44 | R,A | $01257111519202122 \dagger$ |
| 44 | R,S | 01258111417202122 |
| 44 | R,A | $01346111318192122 \ddagger$ |
| 44 | R,S | 01349111318192122 |
| 44 | R,A | $01349111618192122 \ddagger$ |
| 46 | NR,A | 01237111519212224 |
| 46 | NR,A | 01257111519212224 |

Table 1: With length $k=10$, there are eight extremal restricted bases and two extremal nonrestricted bases, listed by Wagstaff [10]. The two bases marked with $\dagger$ are mirror images of each other; similarly the two bases marked with $\ddagger$. Notes: $\mathrm{R}=$ restricted, $\mathrm{NR}=$ nonrestricted; $\mathrm{S}=$ symmetric, $\mathrm{A}=$ asymmetric.
2. If an extremal basis is restricted, is it necessarily symmetric?
3. Does every $k \geq 15$ have an extremal basis that is symmetric?

The first question is answered affirmatively by a theorem of Rohrbach [7]. The second question was posed by Riddell and Chan [6, p. 631], but to our knowledge has not been answered in general; with $k \leq 24$ the answer is yes.

The third question has appeared in a stronger form: it was suggested that all extremal bases with $k \geq 15$ might be symmetric [1]. This was later disproven by Challis and Robinson, since $k=21$ has three extremal bases: one symmetric, two asymmetric [2]. The question remains whether every $k \geq 15$ has at least one extremal basis that is symmetric.

In this work we describe an efficient algorithm for finding all extremal restricted bases of a given length $k$. The algorithm is based on the idea that a restricted basis can be constructed by concatenating two shorter admissible bases, one of them as a mirror image. With this method we have computed all extremal restricted bases of lengths $k \leq 41$.

Note that we have included $a_{0}=0$ in a basis, similarly to Wagstaff [10]. If 0 is excluded, the equivalent condition is that every integer in $[0, n]$ is the sum of at most two elements of the basis [8, p. 3.1]. Excluding the zero is perhaps more usual in current literature, but including it is more convenient for our purposes. The zero element is not counted in the length of a basis.

## 2 Related work

Our search algorithm builds on a combination of existing ideas. Rohrbach discusses symmetric bases, and the proof of his Satz 1 is based on the observation that if a basis is mirrored from $a_{k}$, then its pairwise sums are mirrored from $2 a_{k}[7]$. We shall exploit a generalization of this for asymmetric restricted bases.

Riddell and Chan discuss the connection between symmetric and restricted bases [6]. Mossige notes that symmetric bases $A_{k}$ can be efficiently searched by scanning through admissible bases of length $A_{\lceil k / 2\rceil}$ [5]. For symmetric bases this is sufficient; the second half of a symmetric basis is a mirror image of the first half, and then Rohrbach's theorem ensures that the constructed set $A_{k}$ is a basis for $2 a_{k}$. For asymmetric restricted bases, a similar search can be conducted separately for the two halves of the basis (prefix and suffix). However, since Rohrbach's theorem does not apply to asymmetric bases, the construction does not automatically yield a basis for $2 a_{k}$. This must be checked separately.

The final ingredient is the "gaps test" by Challis [1]. Based on a simple combinatorial argument, it prunes the search tree of admissible bases, if they are required to have a range of at least a given target value $T$. In section 4 we shall prove lower bounds for the ranges of the prefix and the mirrored suffix. With these lower bounds the gaps test prunes the search tree very efficiently.

## 3 Definitions and initial results

If $A$ and $B$ are sets of integers, we define

$$
A+B:=\{a+b: a \in A, b \in B\}
$$

and if $b$ is an integer, we define the mirror image of $A$ with respect to $b$ as

$$
b-A:=\{b-a: a \in A\} .
$$

The set of integers generated by $A$ is

$$
2 A:=A+A=\left\{a+a^{\prime}: a, a^{\prime} \in A\right\} .
$$

It is straightforward to verify that

$$
2(b-A)=2 b-2 A .
$$

By $[c, d]$ we denote the consecutive integers $\{c, c+1, \ldots, d\}$. Now the condition that $A$ is a basis for $n$ is succintly stated as follows:

$$
2 A \supseteq[0, n] .
$$

If $A_{k}=\left\{a_{0}<\cdots<a_{k}\right\}$ is a basis and $i<k$, then $A_{i}=\left\{a_{0}, \ldots, a_{i}\right\}$ is a partial basis. We state without proof three easy observations (see [1] and [8]):

Lemma 1. If a basis is restricted, then it is admissible.
Lemma 2. If a basis is extremal, then it is admissible.
Lemma 3. If a basis $A_{k}$ is admissible, then for all $i<k$ the partial basis $A_{i}$ is admissible, and $a_{i+1} \leq n_{2}\left(A_{i}\right)+1$.

The first question posed in the introduction is now answered by the following theorem, essentially the same as Rohrbach's Satz 1 [7, p. 4].

Theorem 4. If $A_{k}$ is an extremal basis and it is symmetric, then it is restricted.
Proof. Let $a_{k}=\max \left\{A_{k}\right\}$. By Lemma $2, A_{k}$ is admissible; thus $2 A_{k} \supseteq\left[0, a_{k}\right]$. By symmetry $A_{k}=a_{k}-A_{k}$, thus

$$
2 A_{k}=2\left(a_{k}-A_{k}\right)=2 a_{k}-2 A_{k} \supseteq\left[a_{k}, 2 a_{k}\right] .
$$

Combining the above observations we have $2 A_{k} \supseteq\left[0,2 a_{k}\right]$, thus $A_{k}$ is restricted.
Note that if $A_{k}$ is a restricted basis with range $n$, then its largest element is exactly $a_{k}=n / 2$. Exploiting the idea of mirroring from the largest element we obtain the following theorem.

Theorem 5. If $A_{k}$ is a restricted basis with range $n$, then $a_{k}-A_{k}$ is also a restricted basis for $n$.

Proof. Since $A_{k}$ is a basis for $n$, it follows that $2 A_{k} \supseteq[0, n]$. Now

$$
2\left(a_{k}-A_{k}\right)=2 a_{k}-2 A_{k}=n-2 A_{k} \supseteq[0, n],
$$

thus $a_{k}-A_{k}$ is a basis for $n$. Its largest element is $a_{k}-0=a_{k}=n / 2$, thus it is restricted.
Theorem 5 implies that asymmetric restricted bases always form pairs that are mirror images of each other. Two such pairs are seen in Table 1.

## 4 Prefix and suffix of a restricted basis

Let $A_{k}$ be a restricted basis with range $n$ and length $k \geq 3$. Then by Theorem 5 the mirror image $B_{k}=a_{k}-A_{k}$ is also a restricted basis with range $n$. Choose now an arbitrary pivot index $i$ such that $0<i<k-1$. Split $A_{k}$ into a prefix $A_{i}=\left\{a_{0}<\cdots<a_{i}\right\}$ and a suffix $R=\left\{a_{i+1}<\cdots<a_{k}\right\}$. The prefix is a partial basis of $A_{k}$. The suffix can be mirrored from $a_{k}$ to obtain another basis

$$
B_{j}=a_{k}-R=\left\{b_{0}<\cdots<b_{j}\right\},
$$

where $j=k-1-i$, and $b_{h}=a_{k}-a_{k-h}$ for all $0 \leq h \leq j$. Now $B_{j}$ is a partial basis of $B_{k}$.

By Lemma 1 both $A_{k}$ and $B_{k}$ are admissible, and then by Lemma 3

$$
\begin{aligned}
& n_{2}\left(A_{i}\right) \geq a_{i+1}-1, \\
& n_{2}\left(B_{j}\right) \geq b_{j+1}-1 .
\end{aligned}
$$

We have now lower bounds for the ranges $n_{2}\left(A_{i}\right)$ and $n_{2}\left(B_{j}\right)$, but the bounds depend on $a_{i+1}$ and $b_{j+1}$. However, these values can further be bounded from below:

$$
\begin{aligned}
& a_{i+1}=a_{k}-b_{j} \geq a_{k}-\left(n_{2}\left(B_{j-1}\right)+1\right) \geq a_{k}-n_{2}(j-1)-1, \\
& b_{j+1}=a_{k}-a_{i} \geq a_{k}-\left(n_{2}\left(A_{i-1}\right)+1\right) \geq a_{k}-n_{2}(i-1)-1,
\end{aligned}
$$

where $n_{2}(i-1)$ and $n_{2}(j-1)$ are the maximum ranges of bases of lengths $i-1$ and $j-1$, respectively. These maximum ranges are currently known up to length 24 .

Combining these bounds we can state a necessary condition for $A_{k}$ being a restricted basis with range $n$.

Theorem 6. If $A_{k}$ is a restricted basis with range $n$, and $i$ is an index such that $0<i<k-1$, and $i+j=k-1$, then:

1. The prefix $A_{i}$ is an admissible basis such that $n_{2}\left(A_{i}\right) \geq a_{k}-n_{2}(j-1)-2$.
2. The mirrored suffix $B_{j}=a_{k}-\left\{a_{i+1}, \ldots, a_{k}\right\}$ is an admissible basis such that $n_{2}\left(B_{j}\right) \geq$ $a_{k}-n_{2}(i-1)-2$.

Example 7. Let $k=10$ and $n=44$, and choose $i=5$ (thus $j=4$ ). If $A_{10}$ is a restricted basis for 44, then $a_{10}=22$.

Since $n_{2}(3)=8, b_{4}$ cannot be greater than $8+1=9$; in other words, $a_{6}=22-b_{4}$ cannot be smaller than $22-9=13$; thus $n_{2}\left(A_{5}\right) \geq 12$.

Similarly, since $n_{2}(4)=12, a_{5}$ cannot be greater than $12+1=13$; in other words, $b_{5}=22-a_{5}$ cannot be smaller than $22-13=9$; thus $n_{2}\left(B_{4}\right) \geq 8$.

The lower bounds are the ones given by Theorem 6. Consider now a restricted basis $A_{10}$ and its mirror image $B_{10}$, shown in right-to-left order:


The prefix $A_{5}$ has range 12, and the mirrored suffix $B_{4}$ has range 10. Both ranges are within the bounds required by Theorem 6 .

The second part of Theorem 6 also provides an upper bound for the range of a restricted basis:

$$
\begin{aligned}
n_{2}\left(A_{k}\right)=2 a_{k} & \leq 2 n_{2}\left(B_{j}\right)+2 n_{2}(i-1)+4 \\
& \leq 2 n_{2}(j)+2 n_{2}(i-1)+4
\end{aligned}
$$

Choosing $i=\lfloor k / 2\rfloor$ this yields the following bounds, for even and odd values of $k$.
Corollary 8. If $r>1$ is an integer, then

$$
\begin{aligned}
n_{2}^{*}(2 r) & \leq 4 n_{2}(r-1)+4, \\
n_{2}^{*}(2 r+1) & \leq 2 n_{2}(r-1)+2 n_{2}(r)+4 .
\end{aligned}
$$

## 5 Search algorithm

Suppose that $k$ and $n$ are given, and the task is to enumerate every restricted basis of length $k$ and range $n$ (if any such bases exist). Choose a pivot index $i$, for example $i=\lfloor k / 2\rfloor$.

A straightforward method would be to enumerate all admissible prefix bases $A_{i}$, all admissible mirrored suffix bases $B_{j}$, and for each pair $\left(A_{i}, B_{j}\right)$ check whether $A_{i} \cup\left(n / 2-B_{j}\right)$ happens to be a basis for $n$, that is, whether it generates all integers in $[0, n]$. For large $k$ this is not feasible, as the number of admissible bases of length $i$ increases rapidly (see A167809 in [9]).

However, Theorem 6 gives definite lower bounds for the ranges of the prefix $A_{i}$ and the mirrored suffix $B_{j}$. Thus only a tiny fraction of all admissible prefixes and mirrored suffixes need to be considered, as seen in the following example.

Example 9. Let $k=25$ and $n=228$. We want to know whether there are any restricted bases with these values, and to list them if there are. Choose $i=12$ (thus $j=12$ ). The last element of a restricted basis must be $a_{k}=n / 2=114$. There are 15752080 admissible bases of length 12 , but we only need to consider the prefixes $A_{i}$ such that $n_{2}\left(A_{i}\right) \geq$ $114-n_{2}(11)-2=58$; there are only 187 such prefixes.

Admissible bases with a given length and a given minimum range can be enumerated with the algorithm ("K-program") described by Challis [1]. Combining these ingredients we obtain Algorithm 1, which enumerates all restricted bases of given length $k$ and range $n$.

If $n_{2}^{*}(k)$ is not known, Algorithm 1 can be run with different values of $n$, starting from the upper bound for $n_{2}^{*}(k)$ provided by Corollary 8. If no solutions are found, $n$ is then decreased in steps of 2 , until for some $n$ there are solutions. Only even values of $n$ need to be considered, since the range of a restricted basis is always even.

```
Algorithm 1 List restricted bases of length \(k\) and range \(n\)
Require: \(k \geq 3\)
    \(i \leftarrow\lfloor k / 2\rfloor\)
        \{Choose pivot index\}
    \(j \leftarrow k-i-1\)
    \(n_{a} \leftarrow n_{2}(i-1) \quad\) \{Lookup from A001212\}
    \(n_{b} \leftarrow n_{2}(j-1)\)
    \{Lookup from A001212\}
    \(\mathcal{A} \leftarrow\left\{A_{i}: n_{2}\left(A_{i}\right) \geq n / 2-n_{b}-2\right\}\)
\{List prefixes with Challis algorithm [1]\}
    \(\mathcal{B} \leftarrow\left\{B_{j}: n_{2}\left(B_{j}\right) \geq n / 2-n_{a}-2\right\} \quad\) \{List mirrored suffixes with Challis algorithm \(\}\)
    for all \(A_{i} \in \mathcal{A}\) do
        for all \(B_{j} \in \mathcal{B}\) do
            \(R \leftarrow n / 2-B_{j}\)
            \(A_{k} \leftarrow A_{i} \cup R\)
                                    \(\{\) Mirror from \(n / 2\}\)
                            \{Concatenate\}
            if \(2 A_{k} \supseteq[0, n]\) then \(\quad\{\) Generate pairwise sums and check range\}
                print \(A_{k}\)
            end if
        end for
    end for
```

Example 10. Let $k=25$. By Corollary $8, n_{2}^{*}(25) \leq 240$. For $n=240$ the search algorithm finds no solutions. Then $n$ is reduced in steps of 2 , until for $n=228$ the algorithm returns one solution:

$$
\begin{aligned}
& A_{25}=\{0,1,3,4,6,10,13,15,21,29,37,45,53 \\
&61,69,77,85,93,99,101,104,108,110,111,113,114\}
\end{aligned}
$$

By construction, this is an extremal restricted basis, so now we know that $n_{2}^{*}(25)=228$.

## 6 Results

Using the search algorithm described in the previous section, we performed an exhaustive search for extremal restricted bases of lengths $k=25, \ldots, 41$. The bases are listed in Table 3. For ease of reference, previously known extremal restricted bases of lengths $k=1, \ldots, 24$ are listed in Table 2.

For lengths $25, \ldots, 29$ the extremal restricted bases are the extremal symmetric bases listed by Mossige [5]. For lengths $31, \ldots, 41$ they equal the bases given by Challis and Robinson's construction [2, p. 6]. Note that while the aforementioned construction gives a lower bound for the extremal restricted range, exhaustive search gives the exact range.

With $k=30$, there are six extremal restricted bases with range 316. Four of them are symmetric and were listed by Mossige, but two are asymmetric. This is perhaps unexpected, and shows that at least one of the questions 2 and 3 stated in the introduction must be answered negatively. It is currently not known whether $n_{2}(30)$ is 316 or greater.


Table 2: Extremal restricted bases of lengths $k=1, \ldots, 24 . \mathrm{S}=$ symmetric, $\mathrm{A}=$ asymmetric. $+c$ indicates several elements with a repeated difference of $c$.


Table 3: Extremal restricted bases of lengths $k=25, \ldots, 41 . \mathrm{S}=$ symmetric, $\mathrm{A}=$ asymmetric. $+c$ indicates several elements with a repeated difference of $c$.

- If $n_{2}(30)=316$, then we have here two extremal bases that are restricted, but asymmetric; this would answer question 2 negatively.
- If $n_{2}(30)>316$, then there must be some (currently unknown) nonrestricted bases with range greater than 316, but they cannot be symmetric (for if they were, they would be restricted by Theorem 4). This would answer question 3 negatively.

As an example of the time requirement, with $k=41$ and $n=562$, the algorithm generates 5514 prefixes of length 20 and range at least $n / 2-n_{2}(19)-2=139$. These were enumerated in 120 CPU hours on parallel 2.6 GHz Intel Xeon processors, with a C++ implementation of the Challis algorithm. Since 41 is odd, we have $j=i$, and the mirrored suffixes are the same as the prefixes. The concatenation phase of the algorithm (lines 7 to 15) took 1.8 seconds with a Matlab implementation.

## 7 Discussion

Restricted bases are an interesting class of additive bases for two reasons. On one hand, searching for the extremal solutions among restricted bases is enormously faster than searching among all additive bases, as illustrated in the previous sections. This efficiency stems from Theorem 5, which places a very strong constraint on any extremal restricted basis: that its mirror image must also be a restricted basis (possibly different). Thus restricted additive bases can be seen as a generalization of symmetric additive bases.

On the other hand, among lengths $k=1, \ldots, 24$, in almost every case at least one of the extremal bases is restricted (with the sole exception of $k=10$ ). The reason for this is not known, and it is not known whether this regularity continues for $k>24$. The case of $k=30$, discussed in the previous section, suggests that there may be surprises waiting to be found.

For simplicity, we have always taken $i=\lfloor k / 2\rfloor$ in our search algorithm. Further research is needed to find the optimal pivot index $i$ that minimizes the search work.

While Theorem 5 as such does not apply to nonrestricted bases, it would be interesting to know if it could be generalized in such a way that applies to them. Such a generalization might provide an improved search method for extremal additive bases in the nonrestricted case.

## References

[1] M. F. Challis, Two new techniques for computing extremal $h$-bases $A_{k}$, Computer J. 36 (1993), 117-126.
[2] M. F. Challis and J. P. Robinson, Some extremal postage stamp bases, J. Integer Seq. 13 (2010), Article 10.2.3.
[3] J. Kohonen and J. Corander, Addition chains meet postage stamps: Reducing the number of multiplications, J. Integer Seq. 17 (2014), Article 14.3.4.
[4] R. Guy, Unsolved Problems in Number Theory (2004), 2nd edition, SpringerVerlag, pp. 123-127.
[5] S. Mossige, Algorithms for computing the $h$-range of the postage stamp problem, Math. Comp. 36 (1981), 575-582.
[6] J. Riddell and C. Chan, Some extremal 2-bases, Math. Comp. 32 (1978), 630634.
[7] H. Rohrbach, Ein Beitrag zur additiven Zahlentheorie, Math. Z. 42 (1937), 1-30.
[8] E. S. Selmer, The local Postage Stamp Problem. Part 1: General Theory, Technical report no. 42, Department of Pure Mathematics, University of Bergen, 1986.
[9] N. J. A. Sloane, On-Line Encyclopedia of Integer Sequences, http://oeis.org.
[10] S. S. Wagstaff, Additive h-bases for n, in M. B. Nathanson, ed., Number Theory Carbondale 1979, Lect. Notes in Math., Vol. 751, Springer, 1979, pp. 302-327.

2000 Mathematics Subject Classification: Primary 11B13.
Keywords: additive basis, restricted basis.
(Concerned with sequences $\underline{A 001212, ~} \underline{A 006638}$, and $\underline{A 167809 .)}$

